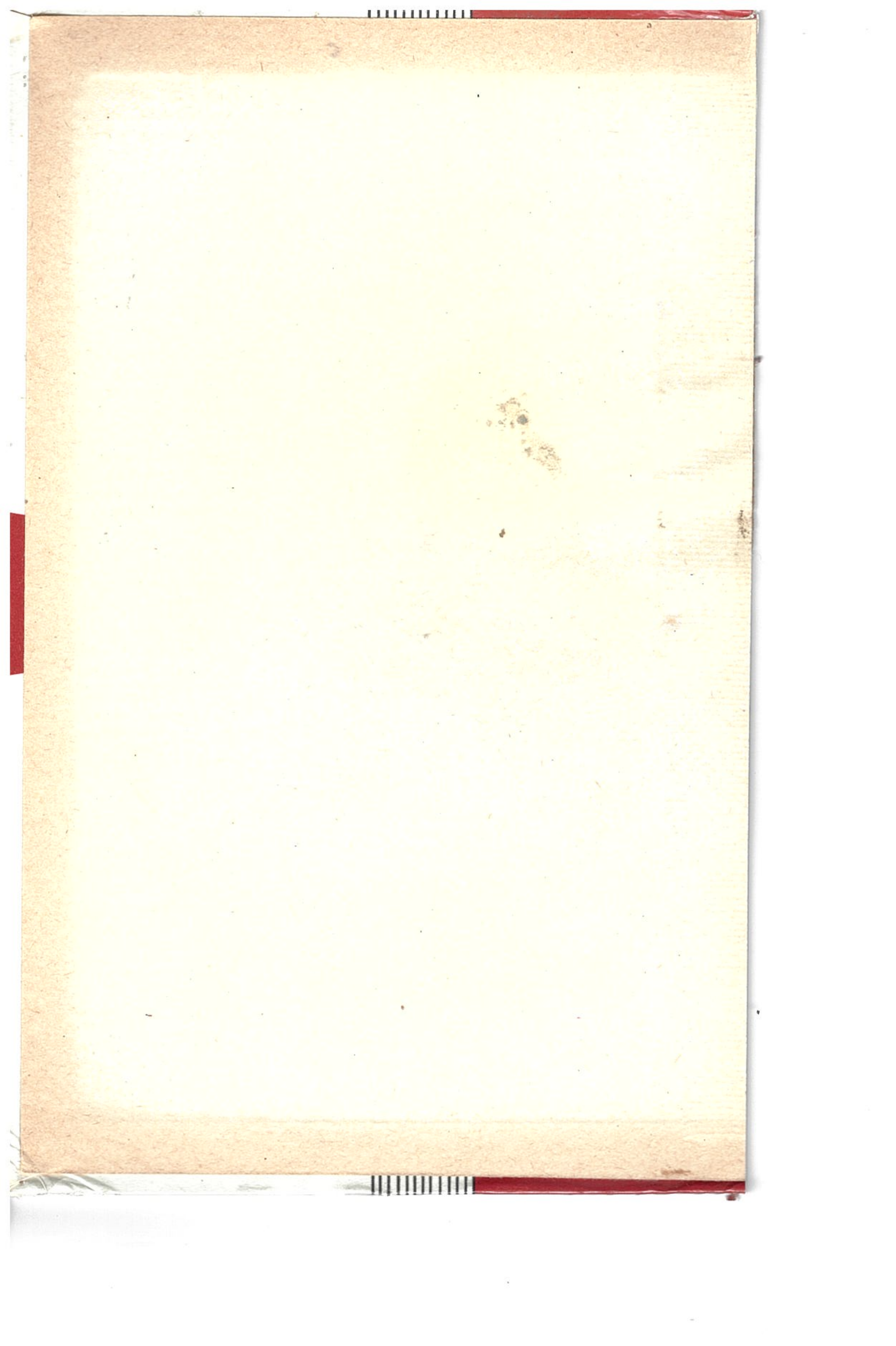
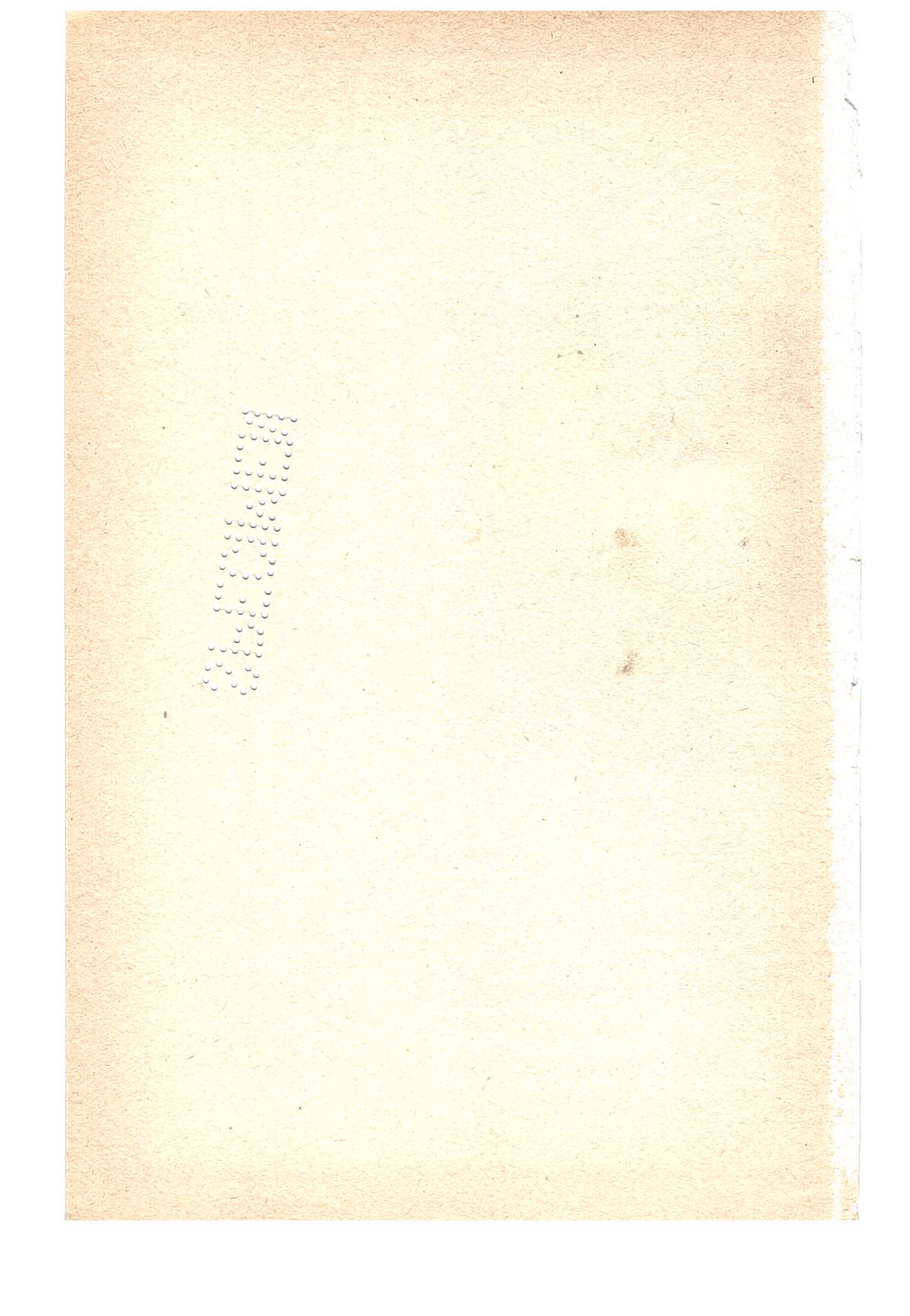
C. BRÉARD

MATHÉMATIQUES ÉLÉMENTAIRES

L'ÉCOLE



Avis Maintenon



C. BRÉARD

MATHÉMATIQUES

CLASSE DE MATHÉMATIQUES ÉLÉMENTAIRES

TOME I

Préface de A. LICHNEROWICZ

2e édition revue

N° 470/1

ÉDITIONS DE L'ÉCOLE
11, rue de Sèvres, PARIS-VIe

DU MÊME AUTEUR

MATHÉMATIQUES, Classe de 6e
MATHÉMATIQUES, Classe de 5e
MATHÉMATIQUES, Classe de 4e
MATHÉMATIQUES, Classe de 3e
MATHÉMATIQUES, Classes de 2e A', C, M, M'
MATHÉMATIQUES, Classes de 2e AB
MATHÉMATIQUES, Classes de 1re A', C, M, M'
MATHÉMATIQUES, Classes de 1re AB

◆

POUR LA MÊME CLASSE

LA PENSÉE ET L'ACTION par **Foulquié.**
PHYSIQUE Collection **Eve-Peschard.**
CHIMIE Collection **Eve-Langlois.**
PROBLÈMES DE PHYSIQUE ET CHIMIE par **Eve.**
CAHIER DE MANIPULATIONS DE PHYSIQUE ET CHIMIE par **Brault-Rey.**
PRÉCIS D'INITIATION AU CINÉMA par **Agel.**

PRÉFACE

Dans le cours de la formation mathématique de chacun de nous, il est des années-clés. Ce sont celles où, après avoir beaucoup travaillé, nous être exercé patiemment sur des chemins variés, nous prenons conscience de nos forces et essayons d'expliciter toutes les convergences perçues en une véritable synthèse rationnelle. Il semble alors que, brusquement, notre intelligence mathématique passe à un autre niveau; l'économie de pensée, obtenue par la mise en évidence de certaines grandes structures, nous permet d'apercevoir, comme d'un coup d'œil, tout le chemin laborieusement parcouru. Elle nous permet aussi la découverte aisée de théories et problèmes nouveaux. Ce sont les années où il semble que chacun participe en esprit, avec quelque bonheur, à ce qu'est la conquête mathématique.

La classe de seconde et la classe terminale nous fournissent des exemples de telles années-clés et c'est ce qu'a bien vu M. Bréard. On sait le succès qu'a rencontré à travers le monde le volume qu'il a consacré à la classe de seconde, volume certes d'abord destiné aux élèves, mais qui par son originalité nous porte aussi, nous professeurs, à maintes réflexions, volume qui peut servir de document de base pour l'élaboration de toute une série d'enseignements à différents niveaux. Qu'il me soit permis d'apporter sur le rayonnement de ce livre un témoignage personnel : lors d'un colloque sur l'enseignement des mathématiques réuni à Bombay, le recteur d'une grande Université russe, mathématicien fort notable, me déclara : « Vous avez en France le livre secondaire le plus moderne du monde; nous nous en servons pour la formation de nos futurs enseignants. » Il s'agissait du livre de seconde de M. Bréard.

Je sais combien le présent volume était attendu. A travers les difficultés qu'il fallait surmonter, la méthode et le talent s'affirment. A ce niveau M. Bréard a tenu à donner un exposé relativement détaillé de la théorie des ensembles, exposé qui précède tout naturellement l'étude de la théorie des nombres. On trouvera ici en particulier une introduction rigoureuse du corps des réels par la méthode des sections commençantes, ainsi qu'une introduction purement algébrique du corps des complexes. Dans ce livre, les domaines des grandes structures mathématiques mises en jeu par le programme officiel sont volontairement séparés, ordonnés, hiérarchisés. Cela a conduit l'auteur à s'abstenir d'élaborer une axiomatique propre de la géométrie euclidienne, mais à reconstruire cette géométrie à partir des stuctures algébriques et topologiques élémentaires.

Ce sont ces structures mêmes que l'élève sorti du Lycée rencontrera constamment, qu'il se tourne vers l'étude du réel physique ou vers celle des sciences économiques et sociales. Ainsi armé des plus précieux instruments de pensée de notre temps, il affrontera sans peur les disciplines particulières, toujours plus nombreuses, qui ont recours aux mathématiques pour leur élaboration.

André LICHNEROWICZ
Professeur au Collège de France.

SYMBOLES ET NOTATIONS

$\neg$	négation d'une assertion	$\neg A$, non A
$\wedge$	conjonction de deux assertions	$C = A \wedge B$, A et B
$\vee$	disjonction de deux assertions	$D = A \vee B$, A *ou* B (*ou* non exclusif)
$\Rightarrow$	implication	$A \Rightarrow B$, A implique B
$\Leftrightarrow$	réciprocité	$A \Leftrightarrow B$, A équivalent à B
E, ...	ensembles : $E = \{1; 2; 3; 4; 5\}$	ou $E = \{x/x \in A$ *et* $x \in B\}$
$\in$	appartenance	$x \in E$, x est élément de E
$\notin$	non appartenance	$x \notin E$, x n'est pas élément de E
$\subset$	inclusion	$A \subset E$, A inclus dans E
		$E \supset A$, E contient A
$\not\subset$	non inclusion	$A \not\subset B$, A n'est contenu dans B
		$B \not\supset A$, B ne contient pas A
$\emptyset$	ensemble vide; partie vide	
$\mathfrak{P}(E)$	ensemble des parties de E	
$\complement_E(A)$	complémentaire de A par rapport à E	
$\cap$	intersection	$J = A \cap B$, J égal à A inter B
$\cup$	réunion	$R = A \cup B$, R égal à A union B
$\forall$	quantificateur universel	$(\forall x)\,(p)$, tout x possède la propriété p
$\exists$	quantificateur existentiel	$(\exists x)\,(p)$, il existe au moins un x qui possède la propriété p
$E \times F$	produit cartésien de deux ensembles	E croix F
$pr_1\,G$	première projection graphe G	$pr_1\,G = A^*$
$pr_2\,G$	seconde projection graphe G	$pr_2\,G = B^*$
A^*	ensemble de définition d'une correspondance	
B^*	ensemble des valeurs d'une correspondance	
$\bigcap_{i=1}^{i=n} A_i$	intersection d'une famille d'ensembles	
$\bigcup_{i=1}^{i=n} A_i$	réunion d'une famille d'ensembles	
$\overset{-1}{\Gamma}$	correspondance réciproque de la correspondance Γ	
$g_o f = h$	produit de deux correspondances :	g rond f

$x \mathfrak{R} y$ le couple $(x ; y)$ possède la propriété $\mathfrak{R}$
$|$ $a|b$, a divise b ; a est diviseur de b
$x \sim y$, $x = y$, mod $\mathfrak{R}$; x équivalent à y, modulo $\mathfrak{R}$
$x < y$: x antérieur à y
$y > x$: y postérieur à x

$\inf_E X$ ou $\inf X$, borne inférieure de X dans E
$\sup_E X$ ou $\sup X$, borne supérieure de X dans E

$\ast$ astérisque ; étoile ; star
$\top$ truc
$\perp$ antitruc

(symboles de lois de composition)

$x \top x = \overset{2}{\top} x$
$f(\alpha;x) = \alpha.x$ $(\alpha \in \Omega ; x \in E)$ loi de composition externe (α : opérateur)
$\aleph_0$ aleph zéro; cardinal du dénombrable $[\aleph_0 = \text{card}(N)]$
$\mathfrak{C}$ cardinal du continu $[\mathfrak{C} = \text{card}(R)]$
A eq B ou Eq(A ; B) : A équipotent à B
$n!$ factorielle n
A_n^p nombre des arrangements de n éléments pris p à p
P_n nombre des permutations de n éléments $P_n = A_n^n = n!$
C_n^p nombre des combinaisons de n éléments pris p à p $C_n^p = \binom{n}{p}$

$\sum$ symbole de sommation $S = \sum_{i=1} a_i$

div A ensemble des diviseurs de A
$A \wedge B = \Delta$, p.g.c.d. de A et B $\Delta = A \wedge B$, A pgcd B
$A \vee B = \mu$, p.p.c.m. de A et B $\mu = A \vee B$, A ppcm B
$a = b$ mod n; a congru à b. modulo n
$\dot{a} = \text{Cl}(a)$, classe de l'élément a $\dot{a}$; a point
N ensemble des cardinaux finis, ou entiers naturels
Z anneau des entiers rationnels (entiers relatifs)
Z/n ou Z/nZ, anneau des entiers modulo n
Q corps des rationnels
R corps des réels
C corps des complexes
$N^* = N - \{0\}$ $Z^* = Z - \{0\}$ $Q^* = Q - \{0\}$
$R^* = R - \{0\}$ $C^* = C - \{0\}$
$Z_+ = \{x / x \in Z ; x \geqslant 0\}$ Q_+ R_+
$Z_- = \{x / x \in Z ; x < 0\}$ Q_- R_-

$\mathcal{M}_1^3$	ensemble des matrices à 1 colonne et 3 lignes
$\mathcal{B}_0$	$= \{ i; j \}$, base canonique de l'espace K^2
$\mathcal{B}_0$	$= \{ i; j; k \}$, base canonique de l'espace K^3
$F^{\perp}$	ensemble des vecteurs orthogonaux à F
$\mathcal{P}(K)$	anneau des polynômes construits sur K (anneau ou corps K)
$\mathcal{F}$	corps des fractions de polynômes

Relations

[R]	Réflexivité
[S]	Symétrie
[AS]	Antisymétrie
[T]	Transitivité

Lois de composition

[C]	Commutativité
[Dg]	Distributivité à gauche } [D] = [Dg] et [Dd]
[Dd]	Distributivité à droite
[D']	Loi externe distributive pour l'addition dans E
[D'']	Loi externe distributive pour l'addition dans Ω
[A]	Associativité d'une loi interne
[A']	Associativité mixte entre la loi externe et la multiplication dans Ω
[A'']	Associativité mixte entre la loi externe et la multiplication dans E
[N]	Existence d'un neutre
[S]	L'ensemble E est symétrisé

sections minorées

[S1]	$\alpha \neq 0$ et $\alpha \neq Q$
[S2]	$(\forall a)\,(\forall b)\,(a \in \alpha$ et $a \leqslant b \Rightarrow b \in \alpha)$
[S3]	α n'a pas de plus petit élément

distance

[M1]	$d(A; B) = 0 \Leftrightarrow A = B$, axiome de séparation
[M2]	$(\forall A)\,(\forall B)\quad d(A; B) = d(B; A)$, axiome de symétrie
[M3]	$(\forall A)\,(\forall B)\,(\forall C),\quad d(A; B) \leqslant d(A; C) + d(C; B)$, axiome de l'inégalité triangulaire.

PREMIÈRE PARTIE

LA THÉORIE DES ENSEMBLES

LIVRE PREMIER

LA NOTION D'ENSEMBLE

CHAPITRE PREMIER

VOCABULAIRE ET SYMBOLES LOGIQUES

1. Assertion.

Une assertion attribue une qualité ou une propriété à un objet.

◇ *Exemples :* Catherine est jolie.
Jean est fort en mathématiques.
$\frac{3}{4}$ est un nombre entier.
Paris est une ville.

Une assertion est vraie ou fausse.

◇ *Exemples :* « Paris est une ville » est une assertion vraie.
« $\frac{3}{4}$ est un nombre entier » est une assertion fausse.

2. Négation d'une assertion.

Si A est une assertion, la négation de cette assertion se note « ¬ A ».

Le signe ¬ de la négation se lit « non ». En pratique, il est peu utilisé en mathématiques. Au lieu de « ¬A » on écrit « non A ».

◇ *Exemples :*
A : Catherine est jolie.
non A : Catherine n'est pas jolie.
A : 4 est un nombre pair.
non A : 4 n'est pas un nombre pair.

3. Conjonction de deux assertions.

On considère deux assertions A et B.

La conjonction est l'opération logique par laquelle on forme une nouvelle assertion C vraie si les deux assertions A et B sont vraies.

On note :

$$C = A \wedge B.$$

Le signe $\wedge$ de la conjonction se lit « et ». En pratique, il est peu utilisé en mathématiques; au lieu de « $A \wedge B$ » on écrit « A et B ».

◇ *Exemples :*

A : Catherine est jolie;
B : Catherine est grande;
A et B : Catherine est jolie et grande.
A : Jean est fort en algèbre;
B : Jean est fort en géométrie;
A et B : Jean est fort en algèbre et en géométrie.

4. Disjonction de deux assertions.

On considère deux assertions A et B.

La disjonction est l'opération par laquelle, à partir des assertions A et B, on forme une nouvelle assertion D vraie :

si A est vraie;
ou si B est vraie;
ou si A et B sont vraies en même temps.

On note :

$$D = A \vee B.$$

Le signe $\vee$ de la conjonction se lit « ou ». En pratique, il est peu utilisé en mathématiques; au lieu de « $A \vee B$ » on écrit « A ou B ».

Mais il faut remarquer qu'en mathématiques, le « ou » n'est pas exclusif. Lorsqu'on a « A ou B », les deux assertions A, B peuvent être vraies en même temps.

◇ *Exemples :*

A : Jean est blond;
B : Jean est fort en mathématiques;
A ou B : Jean est blond ou est fort en mathématiques.

Les deux assertions A, B peuvent être vraies toutes les deux.

A : Le nombre *m* est divisible par 2;
B : Le nombre *m* est divisible par 3;
A ou B : Le nombre *m* est divisible par 2 ou par 3.

5. Implication.

1° ***Soient deux assertions A et B.***

Si lorsque A est vraie, B est vraie, on dit que A implique B.

On note :

$$A \Rightarrow B.$$

Le signe $\Rightarrow$ de l'implication se lit « implique ».

La première assertion A est l'*hypothèse;* la seconde B, est la *conclusion.*

On dit encore que :

$$A \Rightarrow B$$

est un *théorème.*

2° Lorsque l'assertion A est vraie, l'assertion B peut être vraie ou fausse. *Démontrer l'implication ou le théorème, c'est prouver que si A est vraie, B l'est aussi.*

Si A étant vraie, B est vraie, on dit que l'implication ($A \Rightarrow B$) est vraie;

Si A étant vraie, B est fausse, on dit que l'implication ($A \Rightarrow B$) est fausse.

Un théorème ($A \Rightarrow B$) peut donc être considéré comme une assertion.

3° On a évidemment :

$$[(A \Rightarrow B) \text{ et } (B \Rightarrow C)] \Rightarrow (A \Rightarrow C)$$

Autrement dit *l'implication est transitive.*

C'est cette transitivité qui assure le raisonnement déductif.

On peut schématiser cette transitivité (fig. 5).

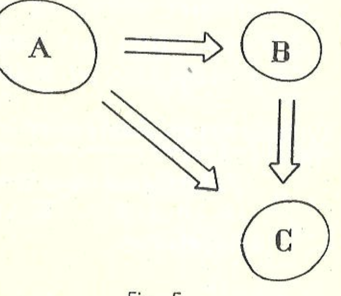


Fig. 5.

4° Il est évidemment très important de s'habituer à écrire un théorème sous forme d'une implication.

◇ *Exemple :* Deux angles droits sont égaux.
A : Deux angles sont droits.
B : Ces deux angles sont égaux.

L'implication donnée : « Deux angles droits sont égaux », s'énoncerait plus clairement :

Si deux angles sont droits, alors ces deux angles sont égaux.

6. Réciprocité.

Soit l'implication A ⇒ B.
L'implication B ⇒ A est l'implication réciproque de la précédente.

L'implication A ⇒ B étant vraie, l'implication B ⇒ A peut être vraie ou fausse.

Lorsque les deux implications sont vraies, on écrit :

$$A \Leftrightarrow B$$

et on lit :

« A implique réciproquement B »

ou :

« A équivalent à B ».

◇ *Exemple 1.*

Soit l'implication :

« Si un nombre est terminé par 5 ou par 0, alors ce nombre est divisible par 5. »

L'implication réciproque est :

« Si un nombre est divisible par 5, alors ce nombre est terminé par 0 ou par 5. »

Cette réciproque est vraie.

◇ *Exemple 2.*

Soit l'implication :

« Si deux angles sont droits, alors ces angles sont égaux. »

L'implication réciproque est :

« Si deux angles sont égaux, alors ces angles sont droits. »

Cette réciproque est fausse.

7. Assertions équivalentes.

Soient deux assertions A et B.
Si on a A ⇔ B, on dit que les deux assertions A et B sont équivalentes.

◇ *Exemple.*

Les deux assertions :

A. Un nombre est terminé par 0 ou par 5,
B. Un nombre est divisible par 5

sont équivalentes.

8. Théories.

En mathématiques, on étudie des théories, c'est-à-dire des successions d'implications.

La théorie des ensembles est la première de ces théories; elle est la base de toutes les mathématiques contemporaines.

A la base d'une théorie on trouve des *termes primitifs;* dans la théorie des ensembles, le terme primitif est le mot « ensemble ».

Dans une théorie, il y a des termes non primitifs : ce sont les *définitions.* Dans la théorie des ensembles, on définit l'intersection, la réunion de deux ensembles, etc...

De plus, on énonce des règles qui permettent d'établir la véracité des implications : ce sont les *schémas de la théorie.*

Enfin, au départ d'une théorie, certaines implications sont supposées exactes : ce sont les *axiomes.*

Une théorie T est contradictoire, si une implication de la théorie est à la fois vraie et fausse.

9. Tiers exclu.

Soit une assertion A.
Si A est vraie, alors non A est fausse.
Si A est fausse, alors non A est vraie.

C'est l'*axiome du tiers exclu.*

◇ *Exemple.*

x étant un nombre entier, ou bien x est pair, ou bien x est impair.

10. Réduction à l'absurde.

1° Soit une théorie T_0 et une assertion A.

On envisage la théorie T obtenue en adjoignant à T_0 l'axiome A, et la théorie T′ obtenue en adjoignant à T_0 l'axiome non A.

Si la théorie T′ est contradictoire, alors A est un théorème de T.

2° Généralement, la démonstration précédente, dite *méthode de réduction à l'absurde,* se présente de la façon suivante :

On suppose que l'assertion A est fausse. On raisonne alors dans la théorie T′ jusqu'à ce qu'on ait montré une contradiction, c'est-à-dire que l'on ait établi à la fois les deux assertions B et non B.

Très souvent B est un théorème de T_0; et lorsque non B est établi, on dit :

« On a B et non B, ce qui est absurde, donc l'assertion A est vraie. »

11. Double négation.

Si A est une assertion de la théorie T, « non non A $\Leftrightarrow$ A » est un théorème de T.

1° Si A est vraie, non A est fausse, et non non A est vraie; donc :

$$A \Rightarrow \text{non(non } A)$$

2° On suppose que non non A est vraie; et on fait une réduction à l'absurde.

Si l'assertion non A est vraie, dans la théorie T′ les assertions non A et non (non A) sont vraies en même temps; ce qui est absurde. Donc A est vraie et :

$$\text{non non } A \Rightarrow A.$$

Finalement, on a l'équivalence :

$$\text{non non } A \Leftrightarrow A.$$

12. Contraposition.

Les deux assertions :

a) A $\Rightarrow$ B

b) non B $\Rightarrow$ non A

sont équivalentes.

1° *a)* $\Rightarrow$ *b)*.

On suppose que A $\Rightarrow$ B est vraie, et que l'assertion non B est vraie. On fait une réduction à l'absurde.

Si A est vraie, alors B est vraie. On a B et non B sont vraies, ce qui est absurde. Donc non A est vraie et :

$$\text{non } B \Rightarrow \text{non } A.$$

2° *b)* $\Rightarrow$ *a)*.

On suppose que non B $\Rightarrow$ non A est vraie, et que l'assertion A est vraie. D'après le 1°, on a :

$$\text{non non } A \Rightarrow \text{non non } B.$$

c'est-à-dire :

$$A \Rightarrow B.$$

3° *Les deux théorèmes (A $\Rightarrow$ B) et (non B $\Rightarrow$ non A) sont dits contraposés. Ils sont équivalents.*

$A \Rightarrow B \Leftrightarrow \overline{B} \Rightarrow \overline{A}$

13. Remarque.

Soient deux assertions A et B, et leurs négations non A et non B. Il est alors possible d'envisager les implications suivantes :

(1) $A \Rightarrow B$ Implication première;
(2) $B \Rightarrow A$ Implication réciproque de l'implication première;
(3) non A $\Rightarrow$ non B Implication inverse de l'implication première;
(4) non B $\Rightarrow$ non A Implication contraposée de l'implication première.

Les implications (1) et (4) sont contraposées donc équivalentes. Il en est de même des implications (2) et (3).

Donc, pour démontrer les quatre implications, il suffit de démontrer (1) et (2). Autrement dit :

$$(A \Leftrightarrow B) \Leftrightarrow (\text{non } A \Leftrightarrow \text{non } B).$$

CHAPITRE II

NOTION D'ENSEMBLE

14. Ensembles.

Le mot « ensemble » est un terme primitif.

Intuitivement, le mot « ensemble » désigne une collection d'objets. Mais ce n'est pas là une définition; un synonyme ne définit pas un autre mot. C'est pour cela que « ensemble » est un terme primitif.

On dira par exemple :

l'ensemble des arbres de la cour;
l'ensemble des doigts de la main;
l'ensemble des nombres pairs.

Un ensemble est souvent désigné par une lettre majuscule E, F... A, B... N, Z, Q, R, C.

Les objets de l'ensemble sont notés par des lettres minuscules a, b, c... x, y... et s'appellent des *éléments* ou des *points de l'ensemble*.

15. Appartenance.

Lorsque l'élément x appartient à l'ensemble E, on note :

$$x \in E$$

Le symbole d'appartenance $\in$ se lit « est un élément de » ou « appartient à ».

Si x n'appartient pas à E, on note :

$$x \notin E$$

et on lit « x n'appartient pas à E », ou « x n'est pas élément de E ».

En fait, il n'y a d'ensemble que dans la mesure où il y a possibilité de savoir si un objet appartient ou non à l'ensemble.

16. Détermination d'un ensemble.

1° Si cela est possible et commode on énonce les éléments qui constituent l'ensemble. C'est la *détermination analytique*.

◇ *Exemples :*

$E = \{ \text{Pierre; Paul; Jacques} \}$
$E = \{ a; e; i; o; u; y \}$
$I = \{ 1; 2; 3; 4; 5 \}$

2° On peut aussi définir les éléments par une propriété permettant de reconnaître sans ambiguïté si un objet appartient ou non à l'ensemble. C'est la *détermination synthétique*.

◇ *Exemples :*

$E = \{ x \,/\, x \text{ est français} \}$
$E = \{ x \,/\, x \text{ est pair} \}$
$E = \{ x \,/\, x \in A \text{ et } x \in B \}$
$E = \{ x \,/\, x \text{ possède la propriété } p \}$
$= E(p)$.

3° On rencontre souvent l'exercice consistant à passer de la forme synthétique à la forme analytique.

◇ *Exemple.* Soit l'équation :

$$x^2 - 3x + 2 = 0.$$

L'ensemble A des solutions est :

$$A = \{ x \,/\, x \in R \quad \text{et} \quad x^2 - 3x + 2 = 0 \}$$

Résoudre l'équation, c'est mettre A sous forme analytique :

$$A = \{ 1; 2 \}$$

17. Diagramme de Venn.

Pour faciliter l'intuition on représente souvent un ensemble par un domaine plan limité par une courbe fermée sans point double : c'est un diagramme de Venn (fig. 17 a).

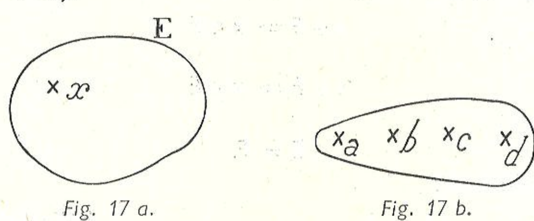


Fig. 17 a. *Fig. 17 b.*

Il est important de remarquer que le dessin n'a aucun rapport avec la nature des éléments de l'ensemble. Cela permettra de comprendre

nettement que les figures de la géométrie ne sont que des diagrammes, mais ne sont pas la géométrie.

Soit l'ensemble :

$$E = \{ a ; b ; c ; d \} ;$$

la figure 17 *b* est le diagramme de cet ensemble.

18. Ensemble vide.

On dit qu'un ensemble E est vide s'il ne contient aucun élément.

On note :

$$E = \varnothing$$

et on lit :

« E est vide »

◇ *Exemples.* Soit E l'ensemble des élèves situés dans la salle de classe; si ces élèves sortent dans la cour de récréation, l'ensemble E est vide.

Soit A l'ensemble des bonbons contenus dans une boîte; on les distribue; à la fin la boîte est vide; l'ensemble A est alors l'ensemble vide.

19. Ensembles ne comprenant qu'un seul élément.

Lorsqu'un ensemble E est constitué par un seul élément x, *on note :*

$$E = \{ x \}.$$

Ceci a pour but de bien mettre en évidence la différence entre l'élément x et l'ensemble $\{ x \}$.

20. Ensembles identiques.

Deux ensembles E et F sont identiques (ou égaux) si tout élément appartenant à l'un appartient à l'autre.

Autrement dit : pour tout x, on a :

$$x \in E \Rightarrow x \in F$$

et

$$x \in F \Rightarrow x \in E$$

On note :

$$E = F.$$

On a évidemment :

$A = A$	Réflexivité.
$(A = B) \Rightarrow (B = A)$	Symétrie.
$[A = B \text{ et } B = C] \Rightarrow (A = C)$	Transitivité.

21. Inclusion.

Soient deux ensembles E et A.

Si tout élément de A est élément de E, on dit que A est inclus dans E.

Autrement dit : pour x, on a :

$$x \in A \Rightarrow x \in E$$

On note :

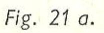
$$A \subset E$$

et on lit :

« A inclus dans E »

ou :

« A contenu dans E ».


Fig. 21 a.

L'écriture $E \supset A$ se lit « E contient A » (fig. 21 *a*).

L'écriture $A \not\subset B$ signifie « A n'est pas contenu dans B ».

◇ *Exemple 1.* Soient :

$$A = \{x \mid x \text{ est pair}\}$$

et :

$$E = N.$$

On a :

$$A \subset N.$$

◇ *Exemple 2.* Soient :

$$A = \{\text{ ensemble des carrés }\}$$

et :

$$E = \{\text{ ensemble des rectangles }\}.$$

On a :

$$A \subset E.$$

◇ *Exemple 3.*

L'ensemble A des nombres divisibles par 3 est contenu dans l'ensemble N des nombres entiers naturels :

$$A \subset N.$$

◇ *Exemple 4.*

Soient A l'ensemble des entiers naturels terminés par 5, et B l'ensemble des entiers divisibles par 5; alors :

$$A \subset B.$$

◇ *Exemple 5.*

Soient un segment AB et deux points A', B' de ce segment (fig. 21 *b*).

A A' B' B

Fig. 21 b.

On a :

$$A'B' \subset AB.$$

◇ *Exemple 6.* Soient les ensembles

$$A = \{1; 2; 4; 6\}$$
$$B = \{1; 2\}$$
$$C = \{2; 3\}$$
$$D = \{1; 2; 4; 6\}$$

On a :

$$B \subset A$$
$$C \not\subset A$$
$$D \subset A \quad \text{avec} \quad D = A.$$

22. Propriétés de l'inclusion.

L'inclusion possède les propriétés suivantes :

Réflexité.

L'inclusion est réflexive.

En effet : pour tout x, on a :

$$x \in A \Rightarrow x \in A$$

donc :

$$A \subset A$$

L'inclusion n'exclut pas l'identité.

Si $A \subset E$ et si $A \neq E$, on dit que l'inclusion est stricte.

Antisymétrie.

L'inclusion est antisymétrique, c'est-à-dire qu'on a l'implication

$$(A \subset B \text{ et } B \subset A) \Rightarrow (A = B).$$

En effet, pour tout x on a :

$$\left[\begin{array}{l} (A \subset B) \Leftrightarrow (x \in A \Rightarrow x \in B) \\ \text{et} \\ (B \subset A) \Leftrightarrow (x \in B \Rightarrow x \in A) \end{array}\right] \Rightarrow (A = B).$$

Transitivité.

L'inclusion est transitive; c'est-à-dire qu'on a l'implication :

$$(A \subset B \text{ et } B \subset C) \Rightarrow (A \subset C)$$

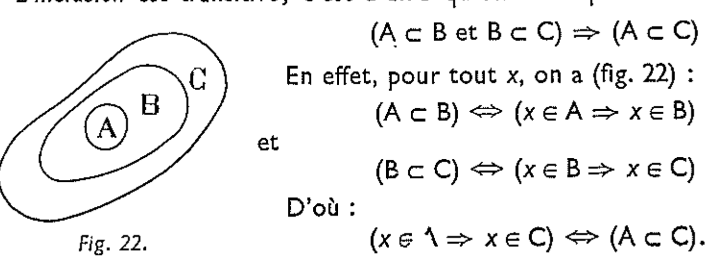


Fig. 22.

En effet, pour tout x, on a (fig. 22) :

$$(A \subset B) \Leftrightarrow (x \in A \Rightarrow x \in B)$$

et

$$(B \subset C) \Leftrightarrow (x \in B \Rightarrow x \in C)$$

D'où :

$$(x \in A \Rightarrow x \in C) \Leftrightarrow (A \subset C).$$

La figure 22 donne l'idée intuitive de la démonstration; elle ne peut pas remplacer cette démonstration.

23. Sous-ensembles.

Si l'ensemble A est contenu dans l'ensemble E on dit que A est un sous-ensemble de E, ou une partie de E.

E est contenu dans E ($E \subset E$), donc E est une partie de E : c'est *la partie pleine de E.*

$\varnothing$ est contenu dans E ($\varnothing \subset E$), donc $\varnothing$ est une partie de E : c'est *la partie vide de E.*

◇ *Exemple.*

Soit $A = \{ 1; 2; 3; 4 \}$

Les ensembles $B = \{ 3; 4 \}$, $C = \{ 2; 4; 3 \}$, A, $\varnothing$ sont des parties de A.

24. Ensemble des parties.

Soit un ensemble E.

On appelle ensemble des parties de E, l'ensemble de tous les sous-ensembles de E, y compris la partie pleine E et la partie vide $\varnothing$.

On note l'ensemble des parties de E : $\mathcal{P}(E)$.

◇ *Exemples.*

1° Soit l'ensemble $A = \{ x \}$.

On a :

$$\mathcal{P}(A) = \{ A; \varnothing \}$$

2° Soit l'ensemble $E = \{ a; b \}$

$$\mathcal{P}(E) = \{ \varnothing; \{ a \}; \{ b \}, E \}$$

3° Soit l'ensemble $E = \{ a; b; c \}$.

On a :

$$\mathcal{P}(E) = \{ \varnothing; \{ a \}, \{ b \}; \{ c \}; \{ a; b \}; \{ a; c \}; \{ b; c \}; E \}.$$

25. Complémentaire d'un ensemble.

1° ***Soit A une partie de l'ensemble E*** (fig. 25).

On appelle complémentaire de A par rapport à E, l'ensemble des éléments de E qui n'appartiennent pas à A.

On note :

$$\complement_E (A)$$

et on a :

$$\complement_E (A) = \{ x \mid x \in E \quad \text{et} \quad x \notin A \}.$$

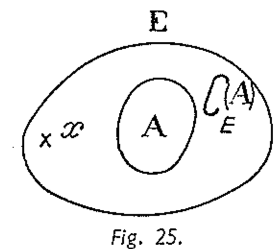


Fig. 25.

◇ *Exemple 1.*

On donne :

A = { 1; 2; 3; 4; 5 } et B = { 2; 4 }.

Donc :

$$\complement_A (B) = \{ 1; 3; 5 \}.$$

◇ *Exemple 2.* Soit A = { x / $x \in$ N et x est pair }.

Alors :

$$\complement_N (A) = \{ x \mid x \in N \quad \text{et} \quad x \text{ est impair} \}.$$

2° On a :

$$\complement_E (E) = \varnothing$$

et

$$\complement_E (\varnothing) = E.$$

26. Intersection de deux ensembles.

On appelle intersection de deux ensembles A et B, l'ensemble J des éléments qui appartiennent à A et à B (fig. 26 *a*).

On note :

J = A ∩ B

et on lit :

J égal à A inter B

On a :

J = A ∩ B = { x / $x \in$ A et $x \in$ B }

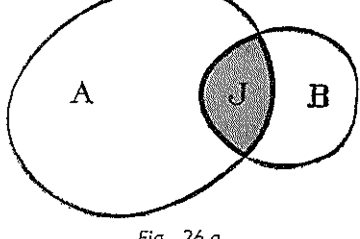


Fig. 26 a.

◇ *Exemple 1.*

1° On donne :

A = { 1; 2; 4; 5; 6 } et B = { 2; 5; 7; 9 }.

On a donc :

A ∩ B = { 2; 5 }.

◇ *Exemple 2.* Soient les deux droites D et D′ de la figure 26 *b*. On a :

$$D \cap D' = \{ A \}.$$

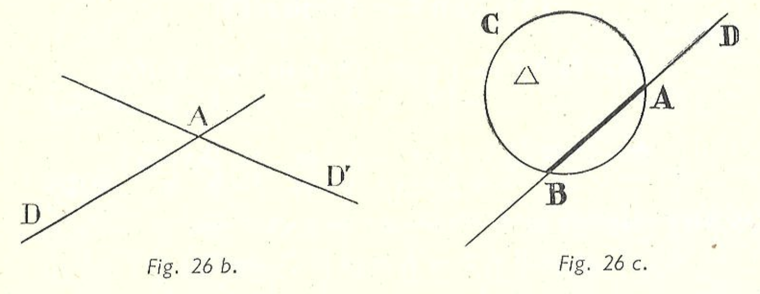


Fig. 26 b. *Fig. 26 c.*

◇ *Exemple 3.* Soient le disque Δ et la droite D de la figure 26 *c*. Leur intersection est le segment AB (ou corde).

$$\Delta \cap D = AB.$$

Mais si sur cette même figure on considère le cercle C frontière du disque Δ, on a :

$$C \cap D = \{ A ; B \}.$$

◇ *Exemple 4.* On considère ici des nombres entiers naturels.

Soient :

$$E = \{ x \mid x \text{ est divisible par } 2 \}$$

et

$$F = \{ x \mid x \text{ est divisible par } 3 \}.$$

Alors :

$$E \cap F = \{ x \mid x \text{ est divisible par } 6 \}.$$

27. Propriétés de l'intersection.

L'intersection possède les propriétés suivantes :

Commutativité.

On a :

$$\boldsymbol{A \cap B = B \cap A}.$$

En effet :

$$A \cap B = \{ x \mid x \in A \quad \text{et} \quad x \in B \}$$

et

$$\begin{aligned} B \cap A &= \{ x \mid x \in B \quad \text{et} \quad x \in A \} \\ &= \{ x \mid x \in A \quad \text{et} \quad x \in B \}. \end{aligned}$$

Les deux résultats sont identiques; on a donc bien $A \cap B = B \cap A$.

Associativité.

On a :

$$(A \cap B) \cap C = A \cap (B \cap C).$$

En effet :

$$\begin{aligned}(A \cap B) \cap C &= \{ x / x \in (A \cap B) \quad \text{et} \quad x \in C \} \\ &= \{ x / x \in A \quad \text{et} \quad x \in B \quad \text{et} \quad x \in C \}\end{aligned}$$

et

$$\begin{aligned}A \cap (B \cap C) &= \{ x / x \in A \quad \text{et} \quad x \in (B \cap C) \} \\ &= \{ x / x \in A \quad \text{et} \quad x \in B \quad \text{et} \quad x \in C \}\end{aligned}$$

Les deux résultats sont identiques; on a donc bien

$$(A \cap B) \cap C = A \cap (B \cap C) \text{ (fig. 27)}.$$

Idempotence.

On a :

$$A \cap A = A.$$

Intersection avec l'ensemble vide.

$$A \cap \varnothing = \varnothing.$$

28. Ensembles disjoints.

Soient deux ensembles A et B (fig. 28 *a*).





Fig. 28 a.

On dit que deux ensembles A et B sont disjoints si leur intersection $A \cap B$ est vide.

$$A \cap B = \varnothing.$$

◇ *Exemples.*

1° Soient

$$A = \{ 1; 2; 3; \} \quad \text{et} \quad B = \{ 5; 6 \}.$$

On a :

$$A \cap B = \varnothing$$

donc A et B sont disjoints.

2° Soient

$$A = \{ 1; 2; 5 \} \quad \text{et} \quad B = \{ 2; 3; 4 \}.$$

On a :

$$A \cap B = \{ 2 \}$$

donc A et B ne sont pas disjoints.

A B A' B'

Fig. 28 b.

3° Les segments AB et A'B' de la figure 28 *b* sont disjoints.

29. Réunion.

On appelle réunion de deux ensembles A et B, l'ensemble R des éléments qui appartiennent à A ou à B (fig. 29).

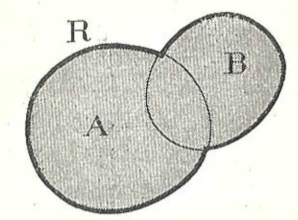


Fig. 29.

On note :

$$R = A \cup B$$

et on lit :

R égal à A union B

On a :

$$A \cup B = \{ x \, / \, x \in A \text{ ou } x \in B \}.$$

◇ *Exemples.*

1° On donne :

$$A = \{ a; b; c \} \quad \text{et} \quad B = \{ e; f \}.$$

On a :

$$A \cup B = \{ a; b; c; e; f \}.$$

2° On donne :

$$A = \{ a; b; c \} \quad \text{et} \quad B = \{ b; c; d; e \}$$

On a :

$$A \cup B = \{ a; b; c; d; e \}.$$

3° Soient A l'ensemble des entiers naturels terminés par 0, et B l'ensemble des entiers naturels terminés par 5 :

$$A = \{ x \, / \, x \text{ est terminé par } 0 \}$$
$$B = \{ x \, / \, x \text{ est terminé par } 5 \}.$$

Alors :

$$A \cup B = \{ x \, / \, x \text{ est terminé par 0 ou par 5} \}$$
$$= \{ x \, / \, x \text{ est divisible par 5} \}.$$

30. Propriétés de la réunion.

La réunion possède les propriétés suivantes :

Commutativité.

On a :

$$\boldsymbol{A \cup B = B \cup A}.$$

En effet :

$$A \cup B = \{ x \, / \, x \in A \text{ ou } x \in B \}$$

et

$$B \cup A = \{ x \, / \, x \in B \text{ ou } x \in A \}$$
$$= \{ x \, / \, x \in A \text{ ou } x \in B \}$$

Les deux résultats sont identiques; on a donc bien $A \cup B = B \cup A$.

Associativité.

On a :

$$(A \cup B) \cup C = A \cup (B \cup C).$$

En effet :

$$(A \cup B) \cup C = \{ x / x \in (A \cup B) \quad \text{ou} \quad x \in C \}$$
$$= \{ x / x \in A \quad \text{ou} \quad x \in B \quad \text{ou} \quad x \in C \}$$

et

$$A \cup (B \cup C) = \{ x / x \in A \quad \text{ou} \quad x \in (B \cup C) \}$$
$$= \{ x / x \in A \quad \text{ou} \quad x \in B \quad \text{ou} \quad x \in C \}$$

Les deux résultats sont identiques; on a donc bien

$$(A \cup B) \cup C = A \cup (B \cup C).$$

Idempotence.

On a :

$$A \cup A = A.$$

Réunion avec l'ensemble vide.

On a :

$$A \cup \varnothing = A.$$

Réunion vide.

On a l'implication évidente

$$(A \cup B = \varnothing) \Rightarrow (A = \varnothing \quad \text{et} \quad B = \varnothing).$$

31. Différence.

Soient deux ensembles A et B.

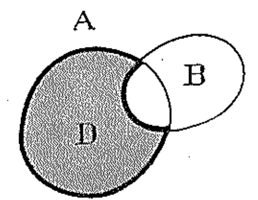


Fig. 31.

On appelle différence de A et B, l'ensemble D des éléments qui appartiennent à A sans appartenir à B (fig. 31).

On note :

$$D = A - B$$

et on a :

$$A - B = \{ x / x \in A \quad \text{et} \quad x \notin B \}.$$

CHAPITRE III

QUANTIFICATION

32. Référentiel.

Très souvent dans une théorie, ou dans une partie d'une théorie, on considère un ensemble d'éléments. Cet ensemble est appelé le *référentiel*. C'est uniquement de ses éléments qu'il est question.

◇ *Exemples :*

L'ensemble N des entiers naturels;
l'ensemble des points du plan;
l'ensemble des triangles.

33. Quantificateurs universel et existentiel.

Soit un ensemble référentiel R et une propriété p. On considère l'ensemble E(p) des éléments de R qui possède la propriété p :

$$E(p) = \{ x \,/\, x \in R \text{ et } x \text{ possède la propriété } p \}$$

Fig. 33 a.

Fig. 33 b.

1° Lorsque E(p) = R, tous les éléments de R possèdent la propriété p (fig. 33 *a*). On peut alors dire :

« quel que soit x, x possède la propriété p »

ou encore

« pour tout x, la propriété p est vérifiée.

On note ces expressions à l'aide du symbole ∀, et on écrit :

$(\forall x)$ (x possède la propriété p)

ou plus brièvement :

$$(\forall x)\ (p)$$

Le symbole $\forall$ se lit « quel que soit... » ou « pour tout... »

$\forall$ est le quantificateur universel.

On a l'équivalence :

$$(\forall x)\ (p) \Leftrightarrow E(p) = R.$$

2° Lorsque l'ensemble $E(p)$ n'est pas vide $E(p) \neq \varnothing$), un élément au moins de R possède la propriété p (fig. 33 *b*). On peut alors dire :

« Il existe un x, au moins, possédant la propriété p ».

On note cette expression à l'aide du symbole $\exists$, et on écrit :

$(\exists x)$ (x possède la propriété p)

ou plus brièvement :

$$(\exists x)\ (p)$$

Le symbole $\exists$ se lit « il existe, au moins, un... »

$\exists$ est le quantificateur existentiel.

On a l'équivalence :

$$(\exists x)\ (p) \Leftrightarrow E(p) \neq \varnothing.$$

34. La négation et les quantificateurs.

1° Lorsque l'ensemble $E(p)$ est vide, $E(p) = \varnothing$, il n'existe aucun élément de R possédant la propriété p.

On note dans ce cas :

$$\text{non } (\exists x)\ (p).$$

Mais dans ce cas le complémentaire de $E(p)$ par rapport à R est R :

$$\complement_R E(p) = R$$

autrement dit tous les éléments de R ne possèdent pas la propriété p; et on note :

$$(\forall x)\ (\text{non } p).$$

Finalement on a l'équivalence :

$$\textit{non } (\exists x)\ (p) \Leftrightarrow (\forall x)\ (\textit{non } p).$$

2° Lorsque $E(p) \neq R$, le complémentaire de $E(p)$ par rapport à R n'est pas vide :

$$\complement_R E(p) \neq \varnothing.$$

Certains éléments de R possèdent la propriété p et certains autres possèdent la propriété non p.
Puisque $E(p) \neq R$ on a non $(\forall x)(p)$, et puisque $\complement_R E(p) \neq \varnothing$, on a $(\exists x)$ (non p).

D'où l'équivalence :

$$\textit{non}\ (\forall x)(p) \Leftrightarrow (\exists x)(\textit{non}\ p).$$

35. La conjonction et les quantificateurs.

1° On a *l'équivalence :*

$$(\forall x)(p \text{ et } q) \Leftrightarrow [(\forall x)(p) \quad \text{et} \quad (\forall x)(q)].$$

En effet, les deux membres de l'équivalence expriment que tous les éléments de R possèdent les propriétés p et q.

On peut aussi remarquer que :

$$E(p \text{ et } q) = E(p) \cap E(q)$$

et que :

$$(\forall x)(p \text{ et } q) \Leftrightarrow [E(p \text{ et } q) = R] \Leftrightarrow [E(p) = E(q) = R].$$

2° On a *l'implication :*

$$(\exists x)(p \text{ et } q) \Rightarrow [(\exists x)(p) \quad \text{et} \quad (\exists x)(q)].$$

Le premier membre exprime que :

$$E(p \text{ et } q) = E(p) \cap E(q) \neq \varnothing.$$

Par suite il existe, au moins, un élément x possédant les propriétés p et q (fig. 35 *a*).

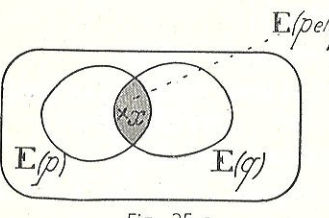


Fig. 35 a.

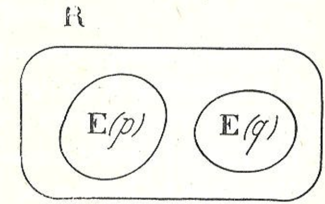


Fig. 35 b.

3° Mais l'implication réciproque de la précédente est fausse.

En effet :

$$[(\exists x)(p) \quad \text{et} \quad (\exists x)(q)]$$

signifie que :

$$E(p) \neq \varnothing \quad \text{et} \quad E(q) \neq \varnothing$$

mais $E(p$ et $q)$ peut être vide si $E(p)$ et $E(q)$ sont disjoints (fig. 35 *b*).

36. La disjonction et les quantificateurs.

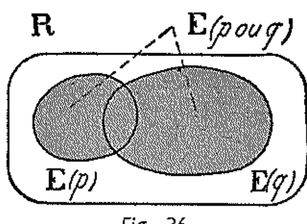


Fig. 36.

On a (fig. 36) :

$$E(p \text{ ou } q) = E(p) \cup E(q).$$

1° On a :

$$[E(p \text{ ou } q) \neq \varnothing] \Leftrightarrow [E(p) \cup E(q) \neq \varnothing].$$

D'où *l'équivalence :*

$$[(\exists x)\ (p \textit{ ou } q)] \Leftrightarrow [(\exists x)\ (p) \textit{ ou } (\exists x)\ (q)].$$

2° On a *l'implication :*

$$[(\forall x)\ (p) \quad \textit{ou} \quad (\forall x)\ (q)] \Rightarrow (\forall x)\ (p \textit{ ou } q).$$

3° Mais l'implication réciproque de la précédente est fausse; en effet

$$(\forall x)\ (p \text{ ou } q) \Leftrightarrow [E(p) \cup E(q) = R]$$

mais cela n'implique pas $E(p) = R$ ou $E(q) = R$.

37. Association des quantificateurs.

1° On a les *équivalences :*

$$(\forall x)\ (\forall y)\ (p) \Leftrightarrow (\forall y)\ (\forall x)\ (p)$$

$$(\exists x)\ (\exists y)\ (p) \Leftrightarrow (\exists y)\ (\exists x)\ (p)$$

2° On a *l'implication :*

$$(\exists x)\ (\forall y)\ (p) \Rightarrow (\forall y)\ (\exists x)\ (p).$$

Mais l'implication réciproque de la précédente est fausse.

Si le référentiel R est l'ensemble des hommes ayant existé ou existant, et la propriété p associée à un couple $(x; y)$ est « x est père de y ».

$(\forall y)\ (\exists x)\ (p)$ signifie « quel que soit y, il existe x père de y ».

Mais $(\exists x)\ (\forall y)\ (p)$ signifie « il existe un homme x, tel que x est le père de tous les y ».

38. Les difficultés de la quantification.

1° *La quantification d'une théorie mathématique n'est pas sans difficultés;* et il y a des précautions à prendre.

Si les quantificateurs sont de même nature, on peut changer leur ordre.

On peut prendre la négation d'une assertion quantifiée assez facilement. Ainsi :

$$(\forall x)\ (\exists y)\ (\forall z)\ (p)$$

a pour négation :

$$(\exists x)\ (\forall y)\ (\exists z)\ (\text{non } p).$$

Il faut, par contre, être très prudent en ce qui concerne la conjonction, la disjonction et la permutation de quantificateurs qui ne sont pas de même nature.

Il y a toute une algèbre de la quantification, et son utilisation n'est pas sans danger.

Par exemple le théorème d'Euclide sur les droites parallèles, se quantifie par

$$(\forall \mathrm{D})\ (\forall \mathrm{A})\ (\exists \mathrm{D}')\ (\mathrm{A} \in \mathrm{D}' \quad \text{et} \quad \mathrm{D} \parallel \mathrm{D}')$$

et il y a déjà trois quantificateurs.

2° *La quantification n'est pas une sténographie;* les symboles $\exists$ et $\forall$ doivent être totalement bannis des textes.

C'est ainsi qu'il est absolument interdit d'écrire des phrases telles que les suivantes :

« La fonction $y = x^2$ est définie $\forall x$ »!

ou

« $\exists$ un triangle ABC ».

De même, la notation

$$\exists x ? \qquad x^2 - 1 = 0$$

ne doit pas être utilisée car le symbole $\exists x ?$ ne peut pas entrer dans l'algèbre des quantificateurs.

CHAPITRE IV

COUPLES

39. La notion de couple.

1° ***Un couple z est l'ensemble de deux éléments x et y donnés dans l'ordre :***

$$z = (x ; y)$$

x est le premier élément, ou première coordonnée, ou première projection;
y est le second élément, ou seconde coordonnée, ou seconde projection.

On note :

$$x = pr_1 z \qquad \text{et} \qquad y = pr_2 z.$$

2° Soient deux couples : $z = (x;\ y)$ et $z' = (x';\ y')$.

Par définition :

$$(z = z') \Leftrightarrow [x = x' \quad \text{et} \quad y = y'].$$

3° On peut généraliser, et parler d'un triplet :

$$u = (x; y; z)$$

ou d'un n-tuple :

$$u = (x_1; x_2; \ldots; x_n).$$

40. Produit cartésien de deux ensembles.

1° ***Soient deux ensembles E et F.***

On appelle produit de E par F, l'ensemble de tous les couples formés de deux éléments x et y, dont le premier appartient à E et le second à F.

On note :

$$E \times F$$

et on lit :

E croix F.

On a :

$$(x; y) \in E \times F \Leftrightarrow (x \in E \text{ et } \quad y \in F).$$

◇ *Exemple. Soient les deux ensembles* $E = \{a; b; c\}$ *et* $F = \{1; 2\}$. *Etudier* $E \times F$.

On a immédiatement :

$$E \times F = \{ (a; 1); (a; 2); (b; 1); (b; 2); (c; 1); (c; 2) \}.$$

2° On peut généraliser et parler de $E \times F \times G$ ou même de $E_1 \times E_2 \times \ldots \times E_n$.

Ainsi il sera question de R^3 et de R^n, R désignant l'ensemble des nombres réels.

41. Diagramme du produit cartésien de deux ensembles.

On peut représenter $E \times F$ par un diagramme. Ainsi le produit $E \times F$ de l'exemple précédent est représenté par la figure 41 *a*.

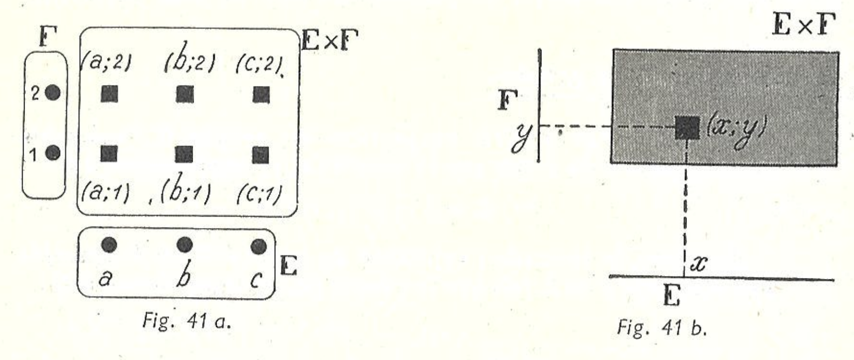


Fig. 41 a.

Fig. 41 b.

De façon générale, un produit cartésien est représentable par un diagramme, tel que celui de la figure 41 *b*.

42. Graphe.

1° *Soient deux ensembles A et B et leur produit cartésien* $A \times B$.

On appelle graphe G un sous-ensemble du produit $A \times B$.

C'est donc l'ensemble des couples $(x; y)$ qui constitue ce sous-ensemble de $A \times B$. La figure 42 *a* représente le diagramme de ce graphe G ou la représentation graphique du graphe.

◇ *Exemple.* Soient $A = \{a; b; c\}$ et $B = \{1; 2\}$.

$$G = \{ (a; 1); (b; 1); (c; 1); (c; 2) \}$$

un graphe : $G \subset A \times B$.

La figure 42 *b* donne le diagramme de ce graphe.

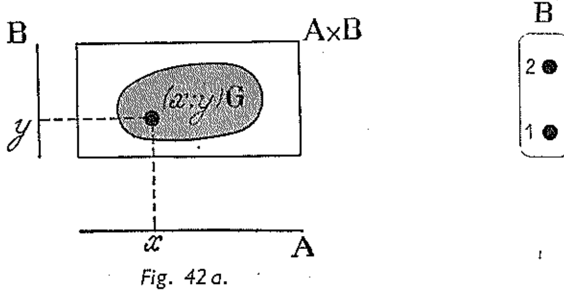


Fig. 42 a.

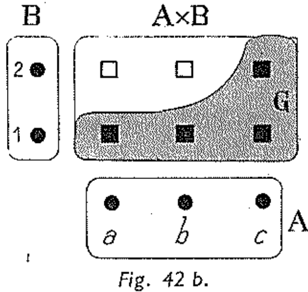


Fig. 42 b.

2° Si le couple $(x; y)$ appartient au graphe G, on dit que y correspond à x par G. On dit aussi que x et y sont liés par une relation *binaire*, parce que G est une partie du produit cartésien de *deux* ensembles.

43. Projection d'un graphe.

On appelle* première projection *du graphe G l'ensemble des éléments x de A tels que le couple (x; y) appartienne à G :

$$\text{pr}_1\, G = \{\, x / (x; y) \in G \,\}$$

De même, la* seconde projection *du graphe G est l'ensemble des éléments y de B tels que le couple (x, y) appartienne à G :

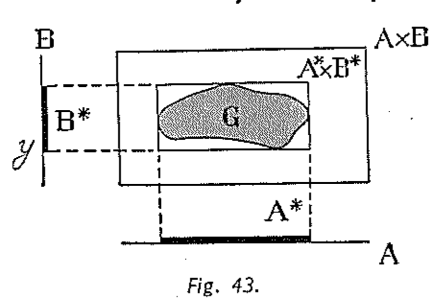


Fig. 43.

$$\text{pr}_2\, G = \{\, y / (x; y) \in G \,\}.$$

On note souvent :

$$\text{pr}_1\, G = A^*$$
$$\text{pr}_2\, G = B^*$$

La figure 43 met en évidence les deux projections du graphe G. On voit alors facilement que

$$G \subset A^* \times B^* \subset A \times B.$$

44. Coupes d'un graphe.

Soit x_0 un élément de A.

On appelle coupe du graphe G suivant x_0, l'ensemble des couples $(x_0; y)$ tels que ces couples appartiennent à G :

$$C(x_0) = \{\, (x_0; y) / (x_0; y) \in G \,\}.$$

Evidement :

$$C(x_0) \neq \varnothing \quad \text{si} \quad x_0 \in A^* \quad \text{et} \quad C(x_0) = \varnothing \quad \text{si} \quad x_0 \in \complement_A(A^*).$$

La figure 44 *a* montre la coupe de G suivant x_0.

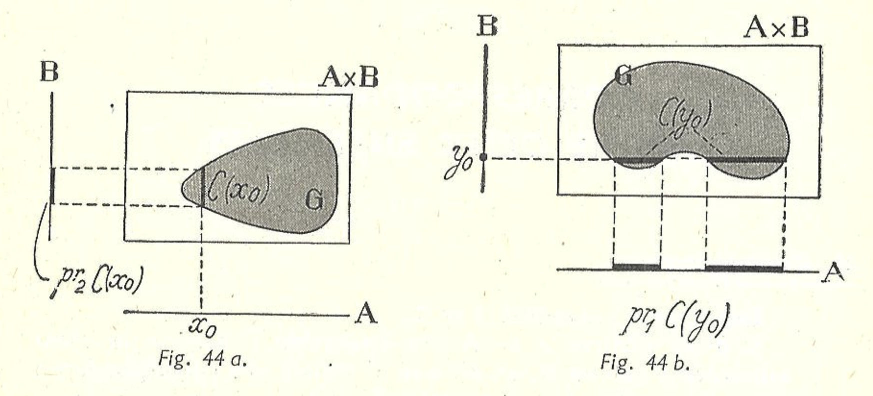


Fig. 44 *a*.

Fig. 44 *b*.

De même, la coupe de G suivant y_0 ***est l'ensemble des couples*** $(x; y_0)$ ***qui appartiennent à G :***

$$C(y_0) = \{ x; y_0)/(x; y_0) \in G \}.$$

La figure 44 *b* montre la coupe de G suivant y_0.

CHAPITRE V

CORRESPONDANCES ENTRE DEUX ENSEMBLES

45. Correspondance.

Soient deux ensembles A et B.

Si à un élément x de A une opération Γ associe un sous-ensemble $\Gamma(x)$ de B, on dit que Γ définit une correspondance entre l'ensemble A et l'ensemble B.

On note :

$$\Gamma : \quad x \in A \longrightarrow \Gamma(x) \in \mathcal{P}(B)$$

ou encore :

$$x \longrightarrow \Gamma(x).$$

L'élément x est l'*argument* (ou la *variable*) et $\Gamma(x)$ est l'*image* de x dans la correspondance Γ.

A est l'*ensemble de départ;* B est l'*ensemble d'arrivée.*

L'ensemble $A^* = \{ x \,/\, x \in A \text{ et } \Gamma(x) \neq \varnothing \}$ est l'*ensemble de définition.* On a : $A^* \subset A$.

L'ensemble $B^* = \{ y \,/\, y \in \Gamma(x) \text{ et } x \in A^* \}$ est l'*ensemble des valeurs.* On a : $B^* \subset B$.

On a aussi : $$B^* = \{ \Gamma(x) / x \in A^* \}.$$

◇ *Exemple.*

Soit l'ensemble $A = \{ a; b; c; d \}$ et l'ensemble $B = \{ 1; 2; 3 \}$. Une correspondance f est définie par

$$f: \quad \begin{aligned} a &\longrightarrow f(a) = 2 \\ b &\longrightarrow f(b) = \{ 2; 3 \} \\ c &\longrightarrow f(c) = \{ 2; 3 \}. \end{aligned}$$

L'ensemble de départ est $A = \{ a; b; c; d \}$.
L'ensemble de définition est $A^* = \{ a; b; c \}$.
L'ensemble d'arrivée est $B = \{ 1; 2; 3 \}$.
L'ensemble des valeurs est $B^* = \{ 2; 3 \}$.

46. Diagramme d'une correspondance.

On peut représenter la correspondance Γ à l'aide du diagramme de la figure 46 *a*.

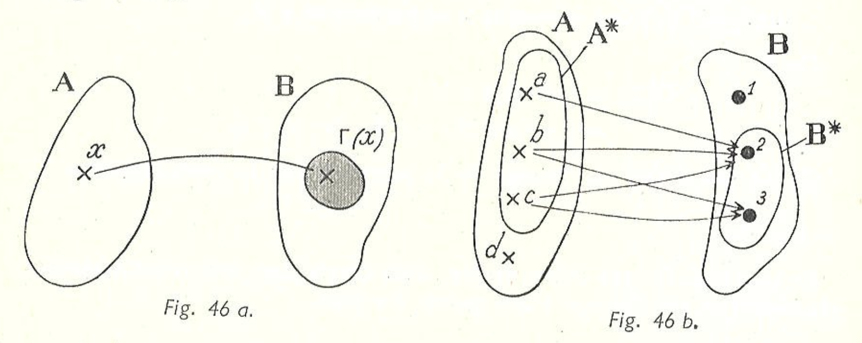


Fig. 46 *a*. Fig. 46 *b*.

Le diagramme de la correspondance f de l'exemple précédent est celui de la figure 46 *b*.

47. Graphe d'une correspondance.

On appelle graphe d'une correspondance l'ensemble des couples (x; y) tels que x ∈ A* et y ∈ Γ(x).

On a :

$$G = \{ (x; y) / x \in A^*; \quad y \in B^*; \quad y \in \Gamma(x) \}.$$

Evidemment :

$$G \subset A^* \times B^* \subset A \times B.$$

◇ *Exemple.*

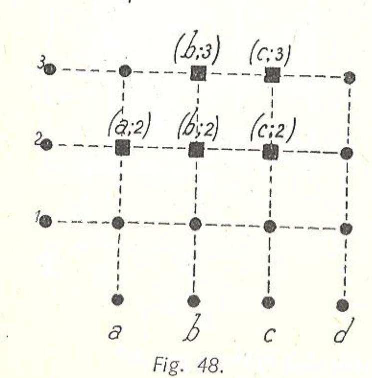


Fig. 48.

Le graphe de la correspondance f du n° 45 est :

$$G = \{ (a; 2); (b; 2); (b; 3); (c; 2); (c; 3) \}.$$

48. Diagramme du graphe d'une correspondance.

Le diagramme du graphe d'une correspondance est la représentation graphique de cette correspondance.

La figure 48 est la représentation graphique de la correspondance f du n° 45.

49. Image d'une partie.

Soit une partie X de A : $X \subset A$.
On désigne par $\Gamma(X)$ le sous-ensemble de B constitué par les images $\Gamma(x)$ des éléments x appartenant à X.

On a :

$$\Gamma(X) = \{ \Gamma(x) / x \in X \}$$
$$= \{ y \,/\, x \in X;\ y \in B;\ (x; y) \in G \}.$$

On dit que $\Gamma(X)$ est l'image de la partie X par la correspondance Γ.

◇ *Exemple.*

En seconde, l'image d'une droite, d'un cercle dans une transformation géométrique est l'image d'une partie du plan.

50. Correspondance réciproque.

A un élément y de l'ensemble B on peut faire correspondre la projection première de la coupe du graphe G de Γ suivant y. On définit ainsi une correspondance entre l'ensemble B et l'ensemble A : c'est la correspondance réciproque de la correspondance Γ.

On la note $\overset{-1}{\Gamma}$ et on a (fig. 50 *a*) :

$$\overset{-1}{\Gamma} : \quad y \in B \longrightarrow \overset{-1}{\Gamma}(y) = pr_1\, C(y).$$

L'ensemble de départ est B; l'ensemble d'arrivée est A.

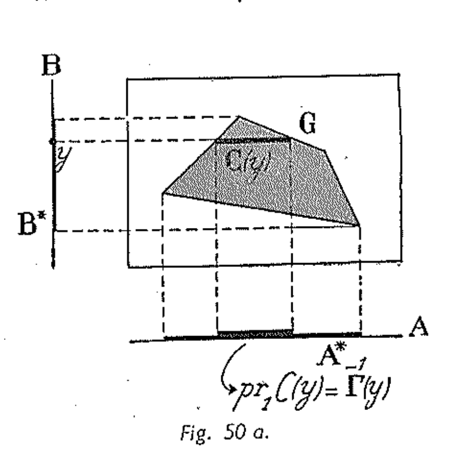


Fig. 50 a.

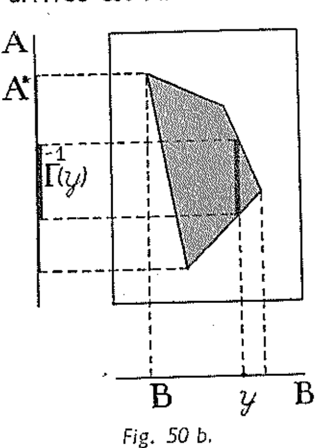


Fig. 50 b.

L'ensemble de définition est B*; l'ensemble des valeurs est A*.

Le graphe $\overset{-1}{G}$ de $\overset{-1}{\Gamma}$ se déduit de G en permutant les rôles de A et B (fig. 50 *b*).

◇ *Exemple.*

La correspondance $\overset{-1}{f}$ réciproque de la correspondance f étudiée au nº 45 est

$$\overset{-1}{f}: \quad 2 \longrightarrow \overset{-1}{f}(2) = \{ a ; b ; c \}$$

$$3 \longrightarrow \overset{-1}{f}(3) = \{ b ; c \}$$

Le graphe de $\overset{-1}{f}$ est donc :

$$\overset{-1}{G} = \{ (2; a); \ (2; b); \ (2; c); \ (3; b); \ (3; c) \}.$$

La représentation graphique est celle de la figure 50 *c*.

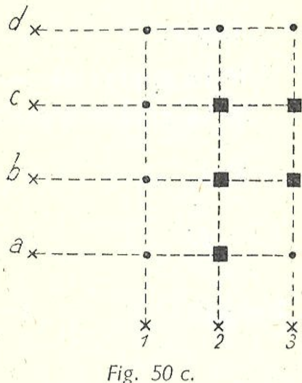


Fig. 50 c.

51. Produit de deux correspondances.

Soient une correspondance f entre les ensembles A et B, et une correspondance g entre les ensembles B et C.

On a :

f : $\quad x \in A \longrightarrow f(x) \subset B$

g : $\quad f(x) \subset B \longrightarrow g[f(x)] \subset C.$

Ainsi à l'élément x de A, on associe une partie $g[f(x)]$ de C. On définit ainsi une correspondance h entre l'ensemble A et l'ensemble C :

h : $\quad x \in A \longrightarrow h(x) = g[f(x)] \subset C.$

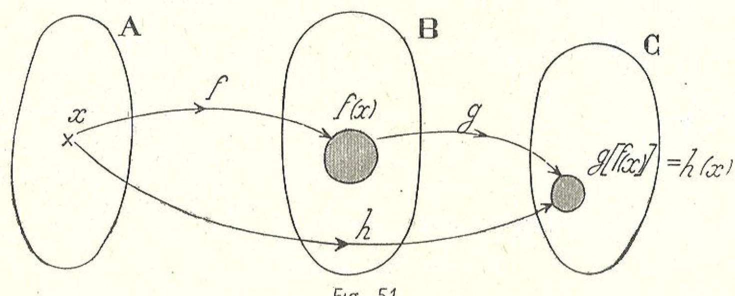


Fig. 51.

La correspondance h *est le produit de la correspondance* f *et de la correspondance* g (fig. 51).

On note :

$$h = g_o f$$

et on lit :

« g rond f ».

◇ *Exemples.*

1° Le produit de deux symétries dans le plan.

2° Le produit d'une isométrie et d'une homothétie.

3° f : $x \longrightarrow u = \sin x.$

g : $u \longrightarrow y = \dfrac{2u - 1}{u + 1}$

$h = g_o f$: $x \longrightarrow y = \dfrac{2 \sin x - 1}{\sin x + 1}.$

52. Correspondance entre un ensemble et lui-même.

1° On peut envisager des correspondances entre l'ensemble A et lui-même (B = A). Ce qui a été dit précédemment est encore valable :

Γ : $x \in A \longrightarrow \Gamma(x) \subset A.$

◇ *Exemple.*

Soit l'ensemble $A = \{ a; b; c; d \}$.

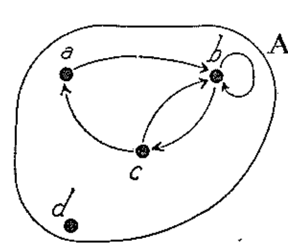


Fig. 52 a.

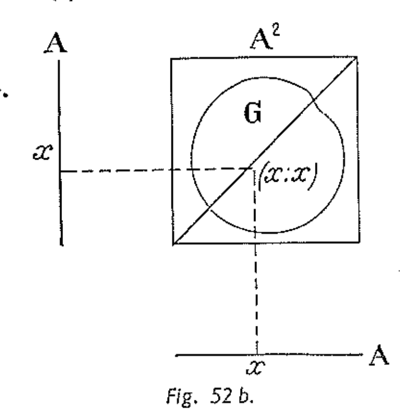


Fig. 52 b.

On définit la correspondance f par :

F : $a \longrightarrow f(a) = b$

$b \longrightarrow f(b) = \{ b ; c \}$

$c \longrightarrow f(c) = \{ a ; b \}.$

Le diagramme de f est donné par la figure 52 *a*.

2° Le graphe G de Γ est une partie de $A \times A = A^2$.

La figure 52 *b* est la représentation graphique de la correspondance *f* de l'exemple précédent.

3° *Lorsque* $\Gamma(x) = x$ *on dit que* x *est invariant.*

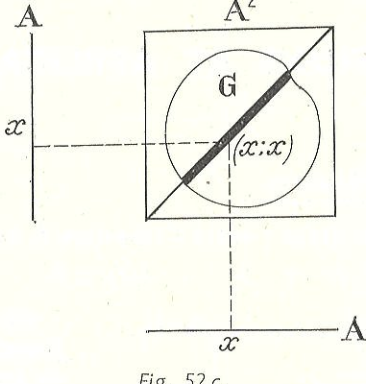


Fig. 52 c.

Les couples tels que $(x;\ x)$ constituent la diagonale D de A^2 (fig. 52 *c*). Les invariants s'obtiennent donc par $pr_1\ (G \cap D)$.

CHAPITRE VI

FONCTIONS ET APPLICATIONS

53. Fonction. Application.

Soit une correspondance f entre l'ensemble A et l'ensemble B :

$$f : \quad x \in A \longrightarrow f(x) \subset B.$$

Fig. 53 a.

On dit que f est une fonction si f(x) contient au plus un élément.

Le graphe correspondant est un graphe fonctionnel.

Lorsque $A^* = A$, on dit que la fonction f est une application.

Une fonction est une application sur A^*. Aussi on identifie souvent fonction et application.

Le graphe [1] de la figure 53 *a* est le graphe d'une fonction; celui de la figure 53 *b* représente une application.

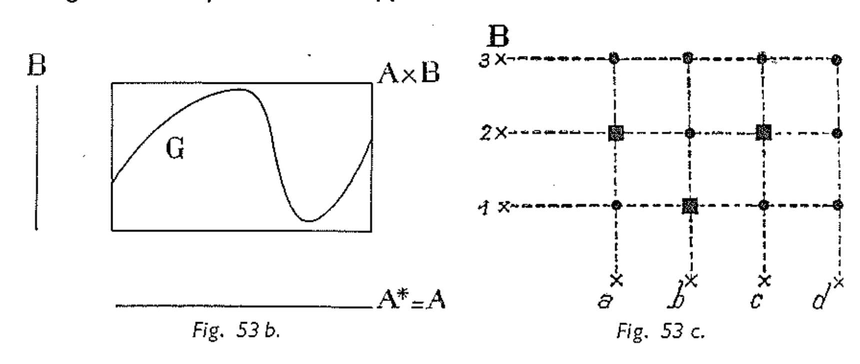


Fig. 53 b. Fig. 53 c.

(1) Par abus de langage on identifie souvent graphe et représentation graphique.

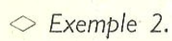
◇ *Exemple 1.*

Soient les ensembles $A = \{ a; b; c; d \}$ et $B = \{ 1; 2; 3 \}$. On définit f par :

$$f: \quad a \longrightarrow f(a) = 2$$
$$b \longrightarrow f(b) = 1$$
$$c \longrightarrow f(c) = 2$$

f est une fonction, car $A^* = \{ a; b; c \}$.

La représentation graphique de f est donnée sur la figure 53 *c*.



◇ *Exemple 2.*

Soient les ensembles $A = \{ a; b; c \}$ et $B = \{ 1; 2; 3; 4 \}$. On définit f par :

$$f: \quad a \longrightarrow f(a) = 2$$
$$b \longrightarrow f(b) = 1$$
$$c \longrightarrow f(c) = 4$$

f est une application, car $A^* = A$.

La représentation graphique de f est donnée sur la figure 53 *d*.

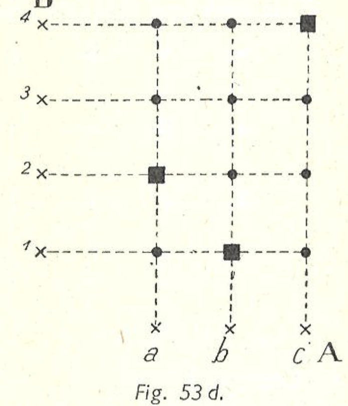


Fig. 53 d.

54. Injection.

Une fonction f est une injection de A dans B si deux éléments distincts de A ont des images distinctes.

On a :

$$x \neq x' \Rightarrow f(x) \neq f(x').$$

Par contraposition, on obtient :

$$f(x) = f(x') \Rightarrow x = x'$$

La figure 54 *a* représente une fonction injective, et la figure 54 *b* une application injective.

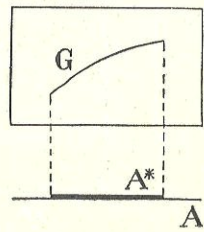


Fig. 54 a.

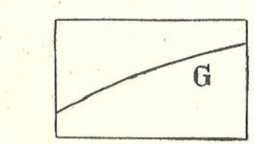


Fig. 54 b.

La coupe du graphe G de f suivant $y \in B$ contient donc au plus un élément.

◇ *Exemple 1.*

Soient $A = \{ a; b; c \}$ et $B = \{ 1; 2; 3 \}$.

On définit la fonction f par :

$$f: \quad a \longrightarrow f(a) = 2$$
$$b \longrightarrow f(b) = 3.$$

La représentation graphique de f est donnée à la figure 54 *c*.
f est bien une fonction injective.

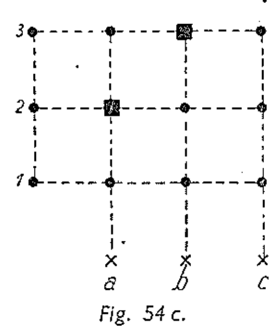


Fig. 54 c.

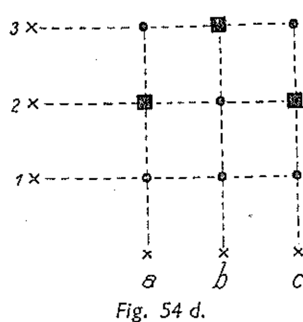


Fig. 54 d.

◇ *Exemple 2.*

Soit la fonction f de A dans B définie par :

$$f: \quad a \longrightarrow f(a) = 2$$
$$b \longrightarrow f(b) = 3$$
$$c \longrightarrow f(c) = 2.$$

La représentation graphique de f est donnée à la figure 54 *d*.
f est une application non injective, car a et c ont la même image 2.

55. Surjection.

Une fonction f est une surjection de A sur B si f (A) = B.

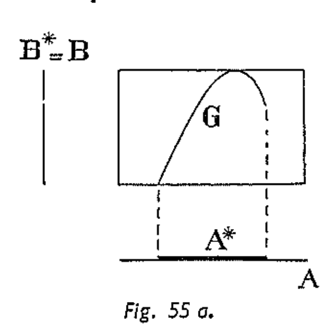


Fig. 55 a.

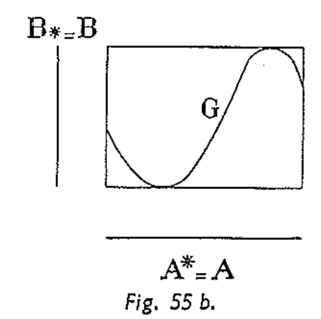


Fig. 55 b.

On a :

$$B^* = B$$

La figure 55 *a* représente une fonction surjective, et la figure 55 *b* une application surjective.

◇ *Exemple.*

Soient les ensembles :

$A = \{ a; b; c; d \}$ et $B = \{ 1; 2; 3 \}$.

On définit une fonction f par :

$$a \longrightarrow f(a) = 2$$
$$b \longrightarrow f(b) = 3$$
$$c \longrightarrow f(c) = 2$$
$$d \longrightarrow f(d) = 1$$

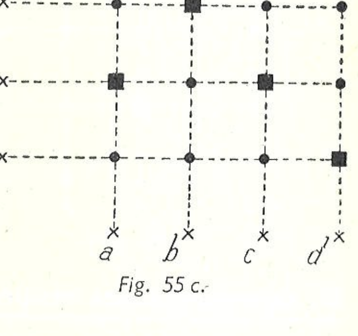


Fig. 55 c.

f est une application surjective de A sur B; elle n'est pas injective. La figure 55 *c* en donne la représentation graphique.

56. Bijection.

Lorsqu'une fonction f est injective et surjective, elle est dite bijective. f est une bijection.

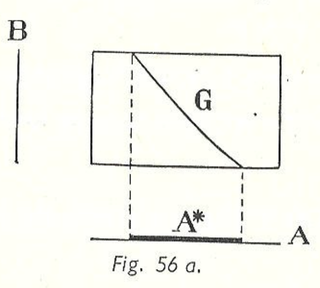


Fig. 56 a.

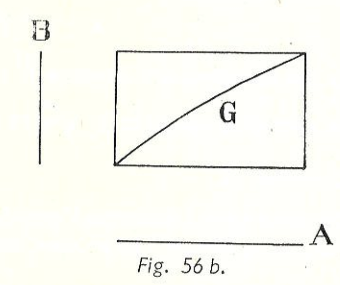


Fig. 56 b.

La figure 56 *a* représente une fonction bijective, et la figure 56 *b* une application bijective.

◇ *Exemple.*

Soient les ensembles $A = \{ a; b; c \}$ et $B = \{ 1; 2; 3 \}$.

On définit une application f par :

f :

$$a \longrightarrow f(a) = 1$$
$$b \longrightarrow f(b) = 3$$
$$c \longrightarrow f(c) = 2.$$

C'est une application bijective de A sur B. La figure 56 c en donne la représentation graphique.

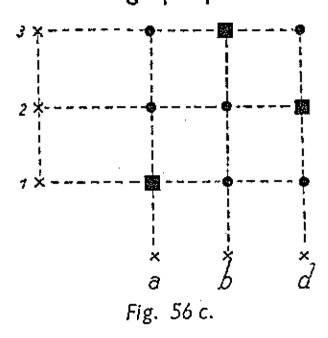


Fig. 56 c.

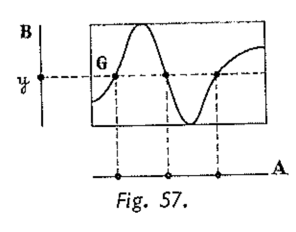


Fig. 57.

57. Correspondance réciproque d'une fonction.

1° *Soit une fonction* f *et son graphe G (fig.* 57). *La coupe* C(y) *de G suivant l'élément* $y \in B$ *contient en général plus d'un élément : il en est de même de* $\overset{-1}{f}(y)$. *Autrement dit,* $\overset{-1}{f}$ *est une correspondance, en général non fonctionnelle entre* B *et* A.

◇ *Exemple 1.*

Soit la fonction f :

f : $$x \longrightarrow f(x) = x^2 = y.$$

La correspondance inverse $\overset{-1}{f}$, à un nombre $y \geqslant 0$ fait correspondre deux nombres opposés $+\sqrt{y}$ et $-\sqrt{y}$; $\overset{-1}{f}$ n'est donc pas une fonction.

◇ *Exemple 2.*

On considère à nouveau l'application f du n° 55 et son graphe (fig. 55 c). La correspondance réciproque est :

$\overset{-1}{f}$:
$$1 \longrightarrow \overset{-1}{f}(1) = d$$
$$2 \longrightarrow \overset{-1}{f}(2) = \{a; c\}$$
$$3 \longrightarrow \overset{-1}{f}(3) = b$$

$\overset{-1}{f}$ n'est donc pas fonctionnelle.

2° C(y) ne contient qu'un seul élément $(x; y)$ si la fonction f est injective car alors y est l'image par f d'un seul élément x; $\overset{-1}{f}(y) = x$.

Donc :

Si la fonction f est injective, sa réciproque $\overset{-1}{f}$ est une fonction.

58. Application réciproque d'une application bijective.

Soit une application bijective f de A sur B.

Puisque f est injective, $\overset{-1}{f}$ est une fonction.

Puisque $B^* = B$, $\overset{-1}{f}$ est une application de B sur A.

Puisque $A^* = A$, $\overset{-1}{f}$ est une surjection.

D'autre part, si $y \neq y'$, on a $\overset{-1}{f}(y) \neq \overset{-1}{f}(y')$ puisque f est injective; donc $\overset{-1}{f}$ est une injection.

Finalement $\overset{-1}{f}$ est une bijection de B sur A.

Et :

Si f est une application bijective de A sur B, alors $\overset{-1}{f}$ est une application bijective de B sur A.

◇ *Exemple.*

On considère à nouveau l'application f de l'exemple du nº 56. f est une bijection de A sur B.

On a :

$\overset{-1}{f}$:

$$1 \longrightarrow \overset{-1}{f}(1) = a$$
$$2 \longrightarrow \overset{-1}{f}(2) = c$$
$$3 \longrightarrow \overset{-1}{f}(3) = b$$

$\overset{-1}{f}$: est bien une application surjective de B sur A.

59. Produit de deux fonctions.

Les résultats suivants sont immédiats :

1º *Le produit de deux fonctions est une fonction.*
2º *Le produit de deux surjections est une surjection.*
3º *Le produit de deux injections est une injection.*
4º *Le produit de deux bijections est une bijection.*

60. Restriction d'une fonction.

Soit une fonction f de A dans B.

On considère une partie X de A ($X \subset A$). La fonction g telle que tout $x \in X$ a pour image $g(x) = f(x)$ est appelée la restriction de f à X.

◇ *Exemple.*

Soient les ensembles $A = \{ a; b; c; d \}$ et $B = \{ 1; 2; 3 \}$.

On considère la fonction f définie par :

$$f : \quad \begin{array}{l} a \longrightarrow f(a) = 2 \\ b \longrightarrow f(b) = 1 \\ c \longrightarrow f(c) = 3 \\ d \longrightarrow f(d) = 2. \end{array}$$

Si $X = \{ a; b; c \}$, la restriction g de f à X est :

$$g : \quad \begin{array}{l} a \longrightarrow g(a) = 2 \\ b \longrightarrow g(b) = 1 \\ c \longrightarrow g(c) = 3 \end{array}$$

Les deux fonctions f et g sont différentes. Ici, en effet, f est une application surjective, non injective de A sur B, tandis que g est une bijection de X sur B.

61. Prolongement d'une application.

Soit une application f de A dans B.

On considère un ensemble X contenant A ($A \subset X$). Toute fonction g définie sur X dont la restriction à A est f est appelée un prolongement de f.

◇ *Exemple 1.*

Soient les ensembles $A = \{ a; b; c \}$ et $B = \{ 1; 2; 3 \}$.

On considère l'application f :

$$f : \quad \begin{array}{l} a \longrightarrow f(a) = 2 \\ b \longrightarrow f(b) = 1 \\ c \longrightarrow f(c) = 3 \end{array}$$

Soit maintenant l'ensemble $X = \{ a; b; c; d \}$; A est une partie de X
On peut envisager la fonction g :

$$g : \quad \begin{array}{l} a \longrightarrow g(a) = f(a) = 2 \\ b \longrightarrow g(b) = f(b) = 1 \\ c \longrightarrow g(c) = f(c) = 3 \\ d \longrightarrow g(d) = 1 \end{array}$$

est un prolongement de f.

Ce n'est pas le seul prolongement possible; ainsi h définie de la façon suivante est aussi un prolongement de f :

h :
$$a \longrightarrow h(a) = f(a) = 2$$
$$b \longrightarrow h(b) = f(b) = 1$$
$$c \longrightarrow h(c) = f(c) = 3$$
$$d \longrightarrow h(d) = 2$$

◇ *Exemple 2.*

La fonction $f : x \longrightarrow f(x) = \frac{\sin x}{x}$ est définie sur $R^* = R - \{ 0 \}$.

Or, on démontre que :

$$\lim_{x=0} \frac{\sin x}{x} = 1.$$

La fonction g telle que :

g :
$$x \in R^* \longrightarrow g(x) = f(x) = \frac{\sin x}{x}$$
$$x = 0 \longrightarrow g(0) = 1$$

est un prolongement de la fonction f, appelé prolongement par continuité parce que g est continue pour $x = 0$.

62. Permutation d'un ensemble.

Toute application bijective f de l'ensemble A sur lui-même s'appelle une permutation de A.

Toute permutation f possède une *permutation réciproque* $\overset{-1}{f}$.

La permutation qui laisse invariant les éléments de A est la *permutation canonique ou l'identité.*

Lorsque $f = \overset{-1}{f}$, la permutation s'appelle une *involution.*

◇ *Exemple.*

Soit l'ensemble $A = \{ a; b; c \}$.

L'application bijective f :

f :
$$a \longrightarrow f(a) = b$$
$$b \longrightarrow f(b) = c$$
$$c \longrightarrow f(c) = a$$

est une permutation de A.

L'identité e est :

e :
$$a \longrightarrow a$$
$$b \longrightarrow b$$
$$c \longrightarrow c$$

63. Fonction de deux arguments.

Soit une fonction f de A dans B.

On suppose que A est le produit de deux ensembles A_1 et A_2. Un élément x de A est donc un couple $(x_1; x_2) \in A_1 \times A_2$.

On a :

$$f: \qquad (x_1; x_2) \in A_1 \times A_2 \longrightarrow f(x_1; x_2) \in B.$$

x_1 et x_2 sont dits les deux arguments; f est une fonction de ces deux arguments.

◇ *Exemple.*

Soit f :

$$f: \qquad (x; y) \in N \times N \longrightarrow f(x; y) = x^y$$

CHAPITRE VII

FAMILLE D'ENSEMBLES

64. Famille d'ensembles.

Soient un ensemble $I \neq \varnothing$ et un ensemble A.

On envisage une application qui à tout $i \in I$ fait correspondre une partie A_i de A :

$$i \in I \longrightarrow A_i \subset A.$$

L'ensemble des images des éléments $i \in I$ est une famille d'ensembles.

On note :

$$\mathcal{A} = \{ A_i / i \in I \}.$$

I s'appelle l'ensemble des indices.

◇ *Exemple.*

Soient :

$$I = \{ \alpha ; \beta ; \gamma \}$$

et

$$A = \{ a ; b ; c ; d ; e \}.$$

On considère :

$$A_\alpha = \{ a ; c ; d \}$$
$$A_\beta = \{ b ; c \}$$
$$A_\gamma = \{ a ; d \}.$$

L'ensemble :

$$\mathcal{A} = \{ A_\alpha ; A_\beta ; A_\gamma \}$$

est une famille d'ensembles, ou une famille de parties de A.

65. Réunion d'une famille d'ensembles.

Soit une famille d'ensembles

$$\mathcal{A} = \{ A_i / i \in I \}$$

On appelle réunion de cette famille l'ensemble des éléments x qui appartiennent à un ensemble au moins de la famille.

On note :

$$\bigcup_{i \in I} A_i = \{ x/(\exists i)\ (i \in I \quad \text{et} \quad x \in A_i) \}.$$

◇ *Exemple.*

En reprenant la famille $\mathcal{A} = \{A_\alpha; A_\beta; A_\gamma\}$ de l'exemple du nº 64, on a :

$$\bigcup_{i \in I} A_i = \{ a ; b ; c ; d \}.$$

66. Intersection d'une famille d'ensembles.

Soit une famille d'ensembles :

$$\mathcal{A} = \{ A_i / i \in I \}.$$

On appelle intersection de cette famille l'ensemble des éléments x qui appartiennent à tous les ensembles de la famille.

On note :

$$\bigcap_{i \in I} A_i = \{ x/(\forall i)\ (i \in I \quad \text{et} \quad x \in A_i) \}.$$

◇ *Exemple.*

Soit la famille $\mathcal{A} = \{ A_\alpha ; A_\beta ; A_\gamma \}$ avec :

$A_\alpha = \{ a ; b ; c \}$ $\quad A_\beta = \{ b ; c ; e ; f \}$ $\quad A_\gamma = \{ a ; b ; c ; f \}$.

On a :

$$\bigcap_{i \in I} A_i = \{ b ; c \}.$$

67. Recouvrement d'un ensemble.

La famille d'ensembles $\mathcal{A} = \{ A_i / i \in I \}$ est un recouvrement de l'ensemble E si $E \subset \bigcup_{i \in I} A_i$.

◇ *Exemple.*

Soient :

$$E = \{ b ; c ; e \}$$

et la famille

$$\mathcal{A} = \{ A_\alpha ; A_\beta ; A_\gamma \}$$

avec

$A_\alpha = \{ a ; b \}$, $\quad A_\beta = \{ a ; b ; d \}$ $\quad A_\gamma = \{ a ; c ; e ; f \}$.

On a :

$$\bigcup_{i \in I} A_i = \{ a ; b ; c ; d ; e ; f \}.$$

Donc :

$$E \subset \bigcup_{i \in I} A_i$$

et par suite $\mathcal{A}$ est un recouvrement de l'ensemble E.

68. Partition d'un ensemble.

Soit une famille $\mathcal{A} = \{ A_i / i \in I \}$ d'ensembles deux à deux disjoints. Cette famille est une partition de l'ensemble E si $E = \bigcup_{i \in I} A_i$.

◇ *Exemple.*

Soient l'ensemble $E = \{ a; b; c; d; e; f \}$

et la famille

$$\mathcal{A} = \{ A_\alpha ; A_\beta ; A_\gamma \}$$

avec

$$A_\alpha = \{ a ; b \} \qquad A_\beta = \{ e \} \qquad A_\gamma = \{ c ; d ; f \}.$$

On a :

$$A_\alpha \cap A_\beta = \varnothing, \quad A_\alpha \cap A_\gamma = \varnothing ; \quad A_\beta \cap A_\gamma = \varnothing$$

autrement dit les ensembles A_i sont deux à deux disjoints. De plus

$$\bigcup_{i \in I} A_i = \{ a ; b ; c ; d ; e ; f \}$$

et

$$E = \bigcup_{i \in I} A_i.$$

Donc, la famille $\mathcal{A}$ est une partition de l'ensemble E.

CHAPITRE VIII

RELATIONS BINAIRES

69. Relation binaire.

Soit un ensemble E. On envisage l'ensemble-produit $E \times E = E^2$. Si une propriété $\mathcal{R}$ peut être associée à un couple $(x; y) \in E^2$ de manière que le couple $(x; y)$ possède la propriété $\mathcal{R}$ ou que le couple $(x; y)$ ne possède pas la propriété $\mathcal{R}$ on dit que $\mathcal{R}$ est une relation binaire.

$\mathcal{R}$ est une relation binaire parce qu'elle est associée à deux éléments x et y de l'ensemble E (1).

Si le couple $(x; y)$ possède la propriété $\mathcal{R}$ on note :

$$\mathcal{R}(x; y)$$

ou plus souvent :

$$x\mathcal{R}y$$

◇ *Exemple.*

1° L'égalité est une relation binaire; au lieu de noter $x\mathcal{R}y$ on note alors :

$$x = y.$$

2° Dans le plan, la relation d'orthogonalité entre les droites est une relation binaire.

On note :

$$D \perp D'$$

3° Dans l'ensemble N des nombres naturels, la relation d'égalité-inégalité, notée $\leqslant$, est une relation binaire :

$$x \leqslant y.$$

---

(1) On peut envisager une relation ternaire; si le triplet $(x; y; z) \in E^3$ possède la propriété $\mathcal{R}$ ou ne possède pas la propriété $\mathcal{R}$.

70. Graphe d'une relation binaire.

◇ *Exemple.*

L'ensemble G des couples (x; y) ∈ E^2 qui possèdent la propriété ℜ est une partie de E^2; c'est le graphe de la relation binaire.

$$G = \{ (x; y) / x\mathfrak{R}y \}$$

◇ *Exemple.*

Dans l'ensemble N, la relation *a* divise *b* est une relation binaire; si *a* divise *b*, ou est diviseur de *b*, on note :

$$a \mid b.$$

Soit l'ensemble :

$$E = \{ 2; 3; 4; 6; 8 \}$$

On a :

2|2	2|4	2|6	2|8
3|3	3|6		
4|4	4|8		
6|6			
8|8			

L'ensemble des couples

(2; 2) (2; 4) (2; 6) (2; 8) (3; 3) (3; 6) (4; 4) (4; 8) (6; 6) (8; 8)

est le graphe G de la relation binaire notée | dans E.

71. Représentation graphique d'une relation binaire.

Le diagramme du graphe G d'une relation binaire est la représentation graphique de cette relation.

◇ *Exemple.*

Le graphe G de la relation binaire dans l'ensemble E de l'exemple précédent a pour diagramme la représentation graphique de la figure 71.

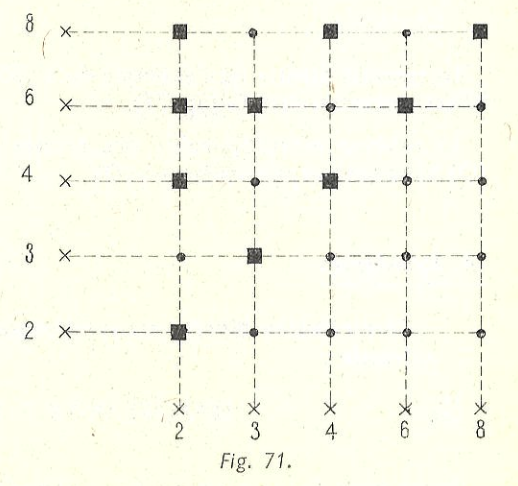


Fig. 71.

72. Relation binaire associée à un graphe.

Soit l'ensemble E^2.

On considère une partie $G \subset E^2$. Un couple $(x; y) \in G$ sera dit posséder la propriété $\mathcal{R}$ et un couple $(x; y) \notin G$ ne possédera pas la propriété $\mathcal{R}$.

On définit ainsi une relation binaire $\mathcal{R}$ dont le graphe est G.

73. Réflexivité.

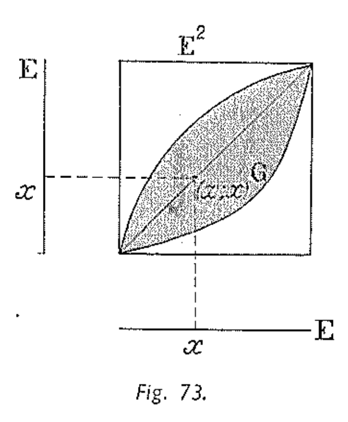


Fig. 73.

Une relation binaire est réflexive si elle possède la propriété suivante :

R $(\forall x) : \quad x \mathcal{R} x.$

Autrement dit, tous les couples $(x; x)$ possèdent la propriété $\mathcal{R}$.

La diagonale de E^2, c'est-à-dire l'ensemble des couples $(x; x)$ est contenue dans le graphe G.

La figure 73 est la représentation graphique d'une relation binaire réflexive.

◇ *Exemples.*

La relation binaire de l'exemple du nº 70 est réflexive; la diagonale de E^2 est contenue dans G (fig. 71).

La relation d'orthogonalité des droites du plan n'est pas réflexive : (D) n'est pas perpendiculaire à (D).

74. Symétrie.

Une relation binaire est symétrique si elle possède la propriété suivante :

S $(\forall x)(\forall y) \quad (x \mathcal{R} y \Rightarrow y \mathcal{R} x).$

Autrement dit, si le couple $(x; y)$ possède la propriété, alors le couple $(y; x)$ possède la propriété.

Si $(x; y)$ appartient à la représentation graphique de G, son symétrique $(y; x)$ pour la diagonale appartient aussi à la représentation graphique (fig. 74).

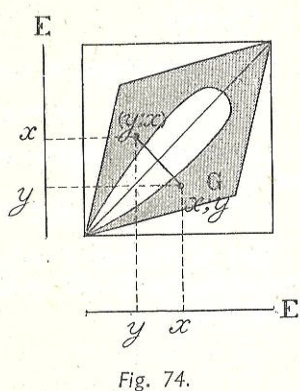


Fig. 74.

◇ *Exemples.*

La relation de divisibilité notée |, déjà envisagée au nº 70, n'est pas symétrique; en effet $4|8$ n'implique évidemment pas $8|4$.

La relation d'égalité, notée =, est symétrique car :

$$(x = y) \Rightarrow (y = x).$$

75. Antisymétrie.

Une relation binaire est antisymétrique si elle possède la propriété suivante :

AS $$(\forall x)\,(\forall y)\,(x \mathcal{R} y \quad \text{et} \quad y \mathcal{R} x) \Rightarrow (x = y)$$

Autrement dit, si le couple $(x; y)$ et le couple $(y; x)$ possèdent la propriété, alors $x = y$.

Le fait que les couples $(x; y)$ et $(y; x)$ possèdent la propriété, n'implique pas que $x = y$ pour toutes les relations. Ainsi, si une relation est symétrique, si $(x; y) \in G$ alors $(y; x) \in G$ et cependant x n'est pas nécessairement identique à y (fig. 74). L'antisymétrie est donc différente de la symétrie.

◇ *Exemples.*

La relation d'égalité-inégalité, notée $\leqslant$, dans N est antisymétrique; en effet :

$$(a \leqslant b \quad \text{et} \quad b \leqslant a) \Rightarrow (a = b)$$

La relation d'inclusion entre les parties d'un ensemble est antisymétrique :

$$(A \subset B \quad \text{et} \quad B \subset A) \Rightarrow A = B.$$

76. Transitivité.

Une relation binaire est transitive si elle possède la propriété suivante :

T $$(\forall x)\,(\forall y)\,(\forall z) : \quad (x \mathcal{R} y \quad \text{et} \quad y \mathcal{R} z) \Rightarrow (x \mathcal{R} z).$$

Cette propriété ne se traduit pas sur la représentation graphique de $\mathcal{R}$.

◇ *Exemples.*

La relation d'égalité, notée =, est transitive, car :

$$(x = y \quad \text{et} \quad y = z) \Rightarrow (x = z).$$

La relation d'inclusion entre les parties d'un ensemble est transitive, car :

$$(A \subset B \quad \text{et} \quad B \subset C) \Rightarrow (A \subset C)$$

Mais la relation d'orthogonalité des droites dans le plan n'est pas transitive, car $D \perp D'$ et $D' \perp D''$ n'implique pas $D \perp D''$ (D et D'' sont parallèles).

CHAPITRE IX

RELATIONS D'ÉQUIVALENCE

77. Relation d'équivalence.

Une relation binaire $\mathfrak{R}$ est une relation d'équivalence si elle est réflexive, symétrique et transitive,

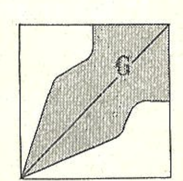
c'est-à-dire si elle possède les trois propriétés suivantes :

R $(\forall x)$: $x \mathfrak{R} x$

S $(\forall x)\,(\forall y)$: $x \mathfrak{R} y \Rightarrow y \mathfrak{R} x$

T $(\forall x)\,(\forall y)\,(\forall z)$: $(x \mathfrak{R} y \quad \text{et} \quad y \mathfrak{R} z) \Rightarrow (x \mathfrak{R} z)$.

La représentation graphique du graphe d'une relation d'équivalence contient la diagonale et est symétrique pour cette diagonale, mais elle ne traduit pas la transivité (fig. 77).



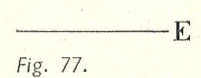


Fig. 77.

◇ *Exemple 1.*

La relation d'égalité, notée $=$, est une relation d'équivalence, car elle possède les trois propriétés suivantes :

R $(\forall x)$: $x = x$

S $(\forall x)\,(\forall y)$: $(x = y) \Rightarrow (y = x)$

T $(\forall x)\,(\forall y)\,(\forall z)$: $(x = y \quad \text{et} \quad y = z) \Rightarrow (x = z)$.

◇ *Exemple 2.*

La relation du parallélisme, au sens large, entre les droites du plan est

une relation d'équivalence, car elle possède les trois propriétés suivantes :

R $(\forall D)$: $D \parallel D$

S $(\forall D)(\forall D')$: $D \parallel D' \Rightarrow D' \parallel D$

T $(\forall D)(\forall D')(\forall D'')$: $(D \parallel D'$ et $D' \parallel D'') \Rightarrow (D \parallel D'')$.

Remarque.

Si $\mathfrak{R}$ est une relation d'équivalence, au lieu de noter $x\mathfrak{R}y$ on note souvent :

$$x \sim y$$

et on lit « x équivalent à y »;

ou :

$$x = y, \text{ mod } \mathfrak{R}$$

et on lit « x égal y, modulo $\mathfrak{R}$ ».

D'autres notations peuvent évidemment être utilisées pour des équivalences particulières; c'est le cas des deux exemples précédents.

78. Classes d'équivalence.

1° Soit un ensemble E muni d'une relation d'équivalence $\mathfrak{R}$.

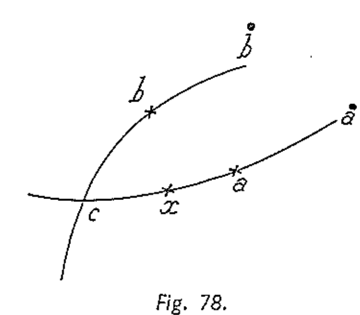


Fig. 78.

On appelle classe d'équivalence selon $\mathfrak{R}$ d'un élément $a \in E$, l'ensemble de tous les éléments x qui sont équivalents à a.

On note :

$$\text{Cl}(a) \text{ ou } \dot{a}$$

et on lit « classe de a » ou « a point »

et :

$$\text{Cl}(a) = \dot{a} = \{x / a\,\mathfrak{R}\,x\}$$

La classe de a est donc une partie de E : $\dot{a} \subset E$.

2° Soient deux éléments a et b de l'ensemble E, et leurs classes d'équivalence $\dot{a} = \text{Cl}(a)$ et $\dot{b} = \text{Cl}(b)$ (fig. 78).

Si ces deux classes ont un élément c en commun, on a :

$$a\mathfrak{R}c \quad \text{et} \quad b\mathfrak{R}c.$$

D'autre part, si x est un élément quelconque de $\dot{a}$

$$a\mathfrak{R}c \quad \text{et} \quad a\mathfrak{R}x \quad \Rightarrow \quad c\mathfrak{R}x$$

et alors

$$b\mathfrak{R}c \quad \text{et} \quad c\mathfrak{R}x \quad \Rightarrow \quad b\mathfrak{R}x$$

ce qui signifie que x appartient à Cl (b). On a donc démontré :

$$(\forall x) \quad x \in \dot{a} \Rightarrow x \in \dot{b}$$

ou encore

$$\dot{a} \subset \dot{b}$$

On démontre de même que :

$$\dot{b} \subset \dot{a}.$$

L'antisymétrie de l'inclusion prouve alors que $\dot{a} = \dot{b}$.

Et :

Si deux classes d'équivalence ont une intersection non vide, alors elles sont identiques.

3° Par contraposition, on obtient :

Si deux classes d'équivalence sont distinctes, alors elles sont disjointes.

Comme tous les éléments de E sont classés :

Les classes d'équivalence sont une partition de l'ensemble.

Evidemment :

Une classe est définie par l'un quelconque de ses éléments :

$$a\mathfrak{R}b \quad \Rightarrow \quad \dot{a} = \dot{b}.$$

79. Ensemble-quotient.

Soit un ensemble E muni d'une relation d'équivalence $\mathfrak{R}$.

L'ensemble des classes d'équivalence est appelé l'ensemble-quotient de E par $\mathfrak{R}$.

On le note :

$$\frac{E}{\mathfrak{R}} \quad \text{ou} \quad E/\mathfrak{R}.$$

◇ *Exemple 1.*

Une classe de jeunes filles comprend les dix élèves suivantes :

Brigitte Bonnet
Catherine Corsage
Corinne Escarpin
Anita Foulard
Antoinette Fourrure
Claudine Manteau
Arlette Mouchoir
Clotilde de Pièce
Sylvie Robe
Béatrice Soulier

Deux élèves seront dites équivalentes si leurs prénoms commencent par la même initiale. (Cette équivalence est immédiate.)

Les classes d'équivalence sont les suivantes :

classe A = { Anita; Arlette; Antoinette }
classe B = { Béatrice; Brigitte }
classe C = { Catherine; Claudine; Corinne; Clotilde }
classe S = { Sylvie }

◇ *Exemple 2.*

On considère l'ensemble Z des entiers rationnels :

$$Z = \{ \dots -n, \dots; -2; -1; 0; 1; 2; \dots, n, \dots \}$$

Deux entiers rationnels sont dits égaux, modulo 3, si leur différence est un multiple de 3 :

$$(a = b, \text{ mod } 3) \Leftrightarrow (a = b + k \cdot 3, \quad k \in Z).$$

C'est une relation d'équivalence, car elle est réflexive, symétrique et transitive.

[R] $(\forall a)\ a = a, \text{ mod } 3$

car :

$$a = a + 0.3.$$

[S] $(\forall a)\ (\forall b)\ (a = b, \text{ mod } 3) \Rightarrow (b = a; \text{ mod } 3)$

car :

$$a = b + k \cdot 3 \Rightarrow b = a + (-k) \cdot 3.$$

[T] $(\forall a)\ (\forall b)\ (\forall c)\ (a = b, \text{ mod } 3 \text{ et } b = c, \text{ mod } 3) \Rightarrow (a = c, \text{ mod } 3)$

car :

$$\left.\begin{array}{r} a = b + k \cdot 3 \\ \text{et} \\ b = c + k' 3 \end{array}\right\} \Rightarrow a = c + (k + k') \cdot 3.$$

Les classes d'équivalence sont alors :

$$\dot{0} = \{ 0; 3; 6; 9; \ldots; -3; -6; -9; \ldots \}$$
$$\dot{1} = \{ 1; 4; 7; 10; \ldots; -2; -5; -8; \ldots \}$$
$$\dot{2} = \{ 2; 5; 8; 11; \ldots; -1; -4; -7; \ldots \}.$$

L'ensemble quotient se note ici Z/3; d'où :

$$Z/3 = \{ \dot{0}; \dot{1}; \dot{2} \}$$

◇ *Exemple 3.*

On considère le plan P privé du point fixe O :

$$P^* = P - \{O\}.$$

Deux points A et B de P* sont liés par la relation binaire $\mathcal{R}$ s'ils sont alignés avec 0.

C'est une relation d'équivalence dans P*, car elle est réflexive, symétrique et transitive.

[R] $(\forall A) : \quad A \mathcal{R} A$

[S] $(\forall A)(\forall B) : \quad A \mathcal{R} B \Rightarrow B \mathcal{R} A$

[T] $(\forall A)(\forall B)(\forall C) : \quad (A \mathcal{R} B \text{ et } B \mathcal{R} C) \Rightarrow (A \mathcal{R} C)$

Les classes d'équivalence sont les droites du plan passant par 0 et privées du point O.

80. Application canonique.

On considère l'application φ qui à un élément x ∈ E fait correspondre la classe d'équivalence de x selon la relation $\mathcal{R}$.

$$\varphi : \quad x \in E \longrightarrow \varphi(x) = Cl(x) = \dot{x} \in E/\mathcal{R}.$$

Cette application est évidemment surjective, mais n'est pas injective (sauf si toutes les classes ne contiennent qu'un élément).

CHAPITRE X

RELATIONS D'ORDRE

81. Relation d'ordre.

Une relation binaire R est une relation d'ordre si elle est réflexive, antisymétrique et transitive,

c'est-à-dire si elle possède les trois propriétés suivantes :

[R] $(\forall x) : \quad x \mathcal{R} x$

[AS] $(\forall x)(\forall y) : \quad (x \mathcal{R} y \quad \text{et} \quad y \mathcal{R} x) \Rightarrow (x = y)$

[T] $(\forall x)(\forall y)(\forall z) : \quad (x \mathcal{R} y \quad \text{et} \quad y \mathcal{R} z) \Rightarrow (x \mathcal{R} z).$

Au lieu de noter $x\mathcal{R}y$, on note généralement une relation d'ordre à l'aide du symbole $\prec$ qui se lit « antérieur à ».

On a alors :

$$x \prec y$$

La relation d'ordre notée $\succ$ (postérieur à) est la relation d'ordre opposée.

82. Eléments comparables. Ordre total. Ordre partiel.

1° ***Soit un ensemble E muni d'une relation d'ordre notée $\prec$. Deux éléments a et b de E sont dits comparables si on a a $\prec$ b ou b $\prec$ a.***

2° ***Si tous les éléments de E sont deux à deux comparables, l'ordre $\prec$ sur E est dit total; et E est un ensemble totalement ordonné. Dans le cas contraire, l'ordre est partiel.***

◇ *Exemple 1.*

Dans l'ensemble N des entiers naturels, on envisage la relation binaire notée $\leqslant$. C'est une relation d'ordre car elle est réflexive, antisymétrique et transitive :

[R] $(\forall x) : \quad x \leqslant x$

[AS] $(\forall x)(\forall y) : \quad (x \leqslant y \quad \text{et} \quad y \leqslant x) \Rightarrow (x = y)$

[T] $(\forall x)(\forall y)(\forall z) \; ; \quad (x \leqslant y \quad \text{et} \quad y \leqslant z) \Rightarrow (x \leqslant z).$

Tous les éléments de N sont deux à deux comparables; si x et y sont deux éléments quelconques de N, on a $x \leqslant y$ ou $y \leqslant x$.

◇ *Exemple 2.*

Soient un ensemble E et l'ensemble $\mathcal{P}(E)$ des parties de E. On envisage dans $\mathcal{P}(E)$ la relation binaire d'inclusion notée $\subset$.

C'est une relation d'ordre car elle est réflexive, antisymétrique et transitive (cf. nº 22).

Si A et B sont deux parties disjointes de $E (A \cap B = \varnothing)$ ces deux éléments ne sont pas comparables, car on a ni $A \subset B$, ni $B \subset A$.

Donc l'inclusion introduit dans $\mathcal{P}(E)$ une structure d'ordre partiel.

83. Fonction croissante. Fonction décroissante.

On envisage une fonction f de l'ensemble A dans l'ensemble B :

$$f : \qquad x \in A \longrightarrow f(x) \in B.$$

On suppose de plus que les ensembles A et B sont totalement ordonnés, les deux ordres étant notés $\prec$.

Soit X une partie de l'ensemble de définition $A^* (X \subset A^*)$.

On dit que la fonction f est croissante sur X si elle possède la propriété suivante :

$$(\forall x)(x \in X), (\forall x')(x' \in X) \quad : \quad x \prec x' \Rightarrow f(x) \prec f(x')$$

On dit que la fonction f est décroissante sur X si elle possède la propriété suivante :

$$(\forall x)(x \in X), (\forall x')(x' \in X) \quad : \quad x \prec x' \Rightarrow f(x') \prec f(x)$$

Dans les deux cas la fonction est dite *monotone sur X*.

◇ *Exemple.*

Soit la fonction :

$$f: \qquad x \in \mathrm{R} \longrightarrow f(x) = x^2 \in \mathrm{R}.$$

C'est une fonction croissante si $x \geqslant 0$, décroissante si $x \leqslant 0$.

84. Plus grand élément. Plus petit élément.

Soit un ensemble E totalement ordonné par la relation notée $\prec$.

1° ***On dit qu'un élément* a $\in$ E *est le plus petit élément de* E *si pour tout* x $\in$ E, *on a* a $\prec$ x.**

Autrement dit :

$$(\forall x)\ (x \in \mathrm{E} \Rightarrow a \prec x) \qquad (84;1)$$

Lorsqu'un ensemble E possède un plus petit élément a, a est unique. En effet, s'il existait un autre plus petit élément b, on aurait :

$$(\forall x)\ (x \in \mathrm{E} \Rightarrow b \prec x) \qquad (84;2)$$

D'après (84; 1) on aurait :

$$a \prec b$$

et d'après (84; 2) :

$$b \prec a$$

L'antisymétrie montre alors que $b = a$.

2° De même :

***On dit qu'un élément* a $\in$ E *est le plus grand élément de* E *si pour tout* x $\in$ E, *on a* x $\prec$ a.**

Autrement dit : $(\forall x)\ (x \in \mathrm{E} \Rightarrow x \prec a)$.

Evidemment, si a existe, il est unique.

◇ *Exemple 1.*

Soit l'ensemble N des entiers naturels.
0 $\in$ N est le plus petit élément de N.
Par contre, N n'a pas de plus grand élément.

◇ *Exemple 2.*

Soit l'ensemble :

$$\mathrm{E} = \left\{ \frac{1}{10^n} \middle/ n \in \mathrm{N} \right\}.$$

Cet ensemble E n'a pas de plus petit élément.
0 n'est pas plus petit élément, car 0 n'appartient pas à E.

85. Majorants. Minorants.

Soit un ensemble E totalement ordonné par la relation notée $\prec$. On considère une partie X de E.

1° ***On appelle minorant de X tout élément a de E tel que pour tout x ∈ X on a a $\prec$ x.***

Autrement dit :

$$(\exists a)\ (a \in E),\ (\forall x)\ (x \in X \Rightarrow a \prec x).$$

Si a est un minorant, et si $a' \prec a$, alors a' est aussi un minorant.

2° ***On appelle majorant de X tout élément a de E tel que pour tout x ∈ A on a x $\prec$ a.***

3° ***Si X est à la fois majoré et minoré, on dit que X est borné.***

◇ *Exemple 1.*

Dans N, on considère X = { 3; 5; 7 }
0; 1; 2, 3 sont des minorants de X.
7, 8, 9,..., sont des majorants de X.
X est donc borné.

◇ *Exemple 2.*

Dans l'ensemble Q des nombres rationnels, on envisage l'ensemble X :

$$X = \left\{ \frac{1}{10^n} \middle/ n \in N \right\}$$

0 est un minorant de X et $0 \notin X$.
1 est un majorant de X et $1 \in X$. (Il est obtenu pour $n = 0$.)

86. Borne supérieure. Borne inférieure.

Soit un ensemble E totalement ordonné par la relation notée $\prec$. On considère une partie X de E.

1° ***On dit qu'un élément de E est la borne inférieure de X dans E si c'est le plus grand élément de l'ensemble des minorants de X.***

On note :

$$\text{Inf}_E X \quad \text{ou} \quad \text{Inf} X.$$

2° ***On dit qu'un élément de E est la borne supérieure de X dans E si c'est le plus petit élément de l'ensemble des majorants de X.***

On note :

$$\text{Sup}_E X \quad \text{ou} \quad \text{Sup} X$$

◇ *Exemple 1.*

Dans N, on considère l'ensemble $X = \{3; 5\}$

On a : $\operatorname{Inf} X = 3$

et : $\operatorname{Sup} X = 5$

◇ *Exemple 2.*

Soit l'ensemble X envisagé à l'exemple 2 du nº 85.

On a : $\operatorname{Inf} X = 0$

et : $\operatorname{Sup} X = 1.$

EXERCICES ET PROBLÈMES SUR LE LIVRE I.

Notion d'ensemble.

1. On donne les deux ensembles A et B. Déterminer $A \cup B$ et $B \cap A$.

$A = \{a; c; d\}$ et $B = \{b; e\}$
$A = \{a; c; e\}$ et $B = \{a; c; e\}$
$A = \{b; c; d\}$ et $B = \{b; d\}$
$A = \{a; c\}$ et $B = \{a; b; c\}$
$A = \{b; d; f\}$ et $B = \{b; c; e\}$

2. On donne les ensembles suivants :

$A = \{a; b; c\}$ $B = \{b; c; d\}$ $C = \{c; d; e\}$ $D = \{d; e; f\}$

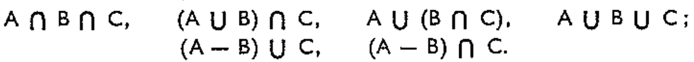
1º Former les ensembles $A \cap B$; $B \cap C$; $A \cap C$.

2º Former les ensembles

$A \cap B \cap C$, $(A \cap B) \cap (C \cap D)$; $(A \cup B) \cap (C \cap D)$.

3. On considère le diagramme de Venn de la figure Ex. 3.
Reproduire cette figure plusieurs fois et hachurer les ensembles suivants :

$A \cap B \cap C$, $(A \cup B) \cap C$, $A \cup (B \cap C)$, $A \cup B \cup C$;


$(A - B) \cup C$, $(A - B) \cap C$.

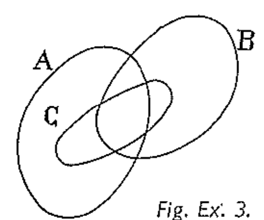


Fig. Ex. 3.

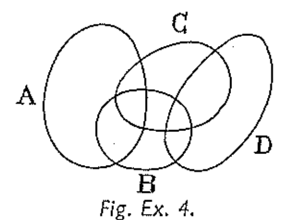


Fig. Ex. 4.

4. On considère le diagramme de Venn de la figure Ex. 4.
Reproduire cette figure plusieurs fois et hachurer les ensembles suivants :

$A \cap B \cap C$, $(A \cup D) \cap (B \cap C)$, $[(A \cup B) - D] \cup C$;
$(A \cap B \cap C) \cup (B \cap C \cap D)$.

5. On considère l'ensemble $E = \{1;2;3;4;5;6\}$ et les deux parties $A = \{1;4;5;6\}$ et $B = \{2;4;6\}$ de cet ensemble.

Déterminer :

$$\complement_E A,\ \complement_E B,\ A \cap B,\ A \cup B,\ A \cap (\complement_E B),\ (\complement_E A) \cap B,\ (\complement_E A) \cup B;$$
$$A \cup \complement_E B,\ (\complement A) \cap (\complement B),\ (\complement A) \cup (\complement B).$$

6. Soit l'ensemble $E = \{1;2;3;4;5;6;7;8;9;10;11;12\}$ et les parties $A = \{1;3;5;7;9;11\}$ et $B = \{2;4;6;8\}$ de cet ensemble.

On pose :

$$\overline{A} = \complement_E A \quad \text{et} \quad \overline{B} = \complement_E B.$$

Former les quatre ensembles :

$$A \cap B,\quad \overline{A} \cap B,\quad A \cap \overline{B},\quad \overline{A} \cap \overline{B}$$

et les quatre ensembles :

$$A \cup B,\quad \overline{A} \cup B,\quad A \cup \overline{B},\quad \overline{A} \cup \overline{B}.$$

7. 1° Soient les deux ensembles $A = \{a;b;c;d\}$ et $B = \{1;2;3\}$

Former les produits cartésiens $A \times B$ et $B \times A$. Tracer les diagrammes représentatifs.

2° On considère $A' = \{a;c;d\}$ et $B' = \{1;2\}$. Former $A' \times B'$. Vérifier que $A' \times B' \subset A \times B$. Diagramme.

8. Soit $A = \{1;2;3\}$. Former $A \times A$. Diagramme représentatif.
Quelle est la diagonale de $A \times A$.

9. On considère l'ensemble $E = \{a;b;c;d;e;f\}$ et les parties $A = \{a;c;d\}$ et $B = \{b;c;f\}$.

Calculer :

$$\overline{A} = \complement_E (A) \quad \text{et} \quad \overline{B} = \complement_E (B)$$
$$\complement_E (A \cap B) \quad \text{et} \quad \complement_E (A \cup B)$$
$$[\complement_E (A \cap B)] \cup [\complement_E A]$$
$$\complement_E (\overline{A} \cap \overline{B}) \quad \text{et} \quad \complement_E (\overline{A} \cup \overline{B})$$
$$(A \cap B) \cup (\overline{A} \cap \overline{B}).$$

10. Soient $A = \{a;b;c\}$ et $B = \{b;c;d\}$.
Former : $A \times A$; $B \times B$; $A \times B$.

Calculer $(A \times A) \cap (B \times B)$; $(A \times A) \cap (A \times B)$; $(B \times B) \cap (A \times B)$.

11. Soient l'ensemble $E = \{1;2;3;4;5;6\}$ et les parties $A = \{1;2;4\}$, $B = \{2;4;5;6\}$, $C = \{1;2;4;5\}$.

Former : $\overline{A} = \complement_E (A)$, $\overline{B} = \complement_E (B)$ et $\overline{C} = \complement_E (C)$.

Calculer ensuite :

$$\alpha = (A \cup B) \cap (\overline{A} \cup B) \cap (A \cup \overline{B})$$
$$\beta = (A \cup B) \cap (A \cup \overline{B}) \cap (\overline{A} \cup \overline{B})$$
$$\gamma = (A \cup B) \cap (\overline{A} \cup B) \cap (\overline{A} \cup \overline{B})$$
$$\delta = (A \cup \overline{B}) \cap (\overline{A} \cup B) \cap (\overline{A} \cup \overline{B})$$

et

$$(A \cup B) \cap (A \cup \overline{B}) \cap (\overline{A} \cup B) \cap (\overline{A} \cup \overline{B}).$$

12. Démontrer les formules suivantes, en utilisant le diagramme de la figure Ex. 12 :

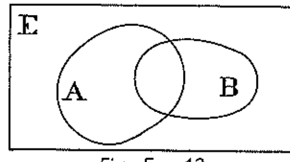


Fig. Ex. 12

$$(A \cap B) \cup B = B$$
$$(A \cup B) \cap B = B$$
$$A \cap (A \cup B) = A$$
$$A \cap [(\complement_E (A) \cup B] = A \cap B$$
$$A \cup [\complement (A) \cap B] = A \cup B.$$

13. Démontrer les formules suivantes (utiliser éventuellement le diagramme figure Ex. 13) :

$$(A \cup B) \cap (B \cup C) \cap (C \cup A) = (A \cap B) \cup (B \cap C) \cup (C \cap A)$$
$$(A \cap C) \cap (B \cup C) = A \cap C$$
$$A \cap C \cap (B \cup \complement_E(C)) = A \cap B \cap C$$
$$(A \cap C) \cup (B \cup C) = B \cup C$$
$$[A \cup \complement(C)] \cap (B \cup C) = (A \cap \complement A) \cup (B \cap C).$$

14. En utilisant le diagramme de la figure Ex. 13, et en posant

$$\overline{A} = \complement_E A, \qquad \overline{B} = \complement_E B, \qquad \overline{C} = \complement_E C$$

démontrer les identités suivantes :

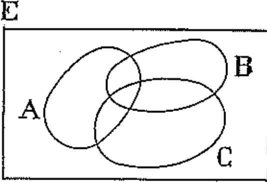


Fig. Ex. 13.

$$(A \cup B) \cap (A \cup \overline{B}) = A$$
$$(A \cup B) \cap (\overline{A} \cup B) = B$$
$$(A \cup B) \cup (\overline{A} \cup \overline{B}) = (A \cap \overline{B}) \cup (B \cap \overline{A})$$
$$(A \cup \overline{B}) \cap (\overline{A} \cup B) = (A \cap B \cup (\overline{A} \cap \overline{B})$$
$$(A \cup \overline{B}) \cap (\overline{A} \cup \overline{B}) = \overline{B}$$
$$(\overline{A} \cup B) \cap (\overline{A} \cup \overline{B}) = \overline{A}$$

15. En utilisant le diagramme de la figure Ex. 13, et en posant $\overline{A} = \complement_E(A)$, $\overline{B} = \complement_E(B)$, $\overline{C} = \complement_E(C)$, montrer que

$$(A \cup B) \cap (A \cup \overline{B}) \cap (\overline{A} \cup B) = A \cap B$$
$$(A \cup B) \cap (A \cup \overline{B}) \cap (\overline{A} \cup \overline{B}) = A \cap \overline{B}$$
$$(A \cup B) \cap (\overline{A} \cup B) \cap (\overline{A} \cup \overline{B}) = \overline{A} \cap B$$
$$(A \cup \overline{B}) \cap (\overline{A} \cup B) \cap (\overline{A} \cup \overline{B}) = \overline{A} \cap \overline{B}$$
$$(A \cup B) \cap (A \cup \overline{B}) \cap (\overline{A} \cup B) \cap (\overline{A} \cap \overline{B}) = \varnothing.$$

16. En utilisant le diagramme de la figure Ex. 13, montrer que

$$(\overline{A} \cap B \cap C) \cup (\overline{A} \cap B \cap \overline{C}) \cup (A \cap B \cap \overline{C}) \cup (A \cap B \cap C) = B \cap (\overline{A} \cup A) = B$$
$$(\overline{A} \cap B \cap C) \cup (A \cap B \cap \overline{C}) \cup (A \cap B \cap C) = \overline{B} \cap A$$
$$(\overline{A} \cap \overline{B} \cap C) \cup (A \cap B \cap \overline{C}) \cup (A \cap \overline{B} \cap \overline{C}) \cup (A \cap \overline{B} \cap \overline{C}) \cup (A \cap \overline{B} \cap C) \cup (A \cap B \cap C) = (A \cup \overline{C}) \cap (\overline{A} \cup \overline{B} \cup C)$$
$$(A \cap B \cap C) \cup (A \cap B \cap \overline{C}) \cup (A \cap \overline{B} \cap C) \cup (A \cap \overline{B} \cap \overline{C}) = A.$$

17. Montrer que la réunion des huit ensembles suivants (fig. Ex. 13)

$$A \cap B \cap C, \quad A \cap \overline{B} \cap C, \quad A \cap B \cap \overline{C}, \quad \overline{A} \cap B \cap C,$$
$$\overline{A} \cap \overline{B} \cap C, \quad \overline{A} \cap B \cap \overline{C}, \quad A \cap \overline{B} \cap \overline{C}, \quad \overline{A} \cap \overline{B} \cap \overline{C}$$

est l'ensemble E.

18. Démontrer l'implication

$(D \subset A, \text{ et } D \subset B, \text{ et } D \subset C \Rightarrow D \subset (A \cap B \cap C)$.

19. Si $A \cap B = A \cap C$, a-t-on $B = C$? Justifier la réponse avec précision.

20. On considère le diagramme de la figure Ex. 13.

On pose :

$$A' = \complement_E A, \quad B' = \complement_E (B), \quad C' = \complement_E (C)$$

et

$$A \star B = (A \cap B) \cup (A' \cap B').$$

Calculer :

$$[(A \star B) \cap (B \star C)] \star [A \star C]$$

21. On donne la propriété

$$\alpha = p \text{ et } q$$

et la propriété

$$\beta = p \text{ ou } q$$

p et q étant des propriétés.

Exprimer les propriétés non α et non β.

Prendre comme exemple :

(p) : le triangle T est isocèle
(q) : le triangle T est rectangle.

22. On considère les propriétés p et q. Montrer que

$$E(p \text{ et } q) \subset E(p)$$
$$E(p \text{ et } q) \subset E(q)$$
$$E(p \text{ ou } q) \supset E(p)$$
$$E(p \text{ ou } q) \supset E(q).$$

Interprétation par un diagramme de Venn.

23. Définir les ensembles suivants par énumération des éléments.

$$A = \{ x / x \in N \quad \text{et} \quad x < 3 \}$$
$$B = \{ x / x \in N \quad \text{et} \quad x^2 < 18 \}$$
$$C = \{ x / x \in N \quad \text{et} \quad x \text{ est pair} \}$$

24. On considère les implications suivantes

1° $(A \subset B \text{ et } B \not\subset C) \Rightarrow (A \not\subset C)$
2° $(A \not\subset B \Rightarrow (B \not\subset A)$
3° $(A \subset B) \text{ et } C \subset B) \Rightarrow [(A \subset B) \text{ ou } (C \subset A)]$
4° $(A \subset B) \Rightarrow (B \not\subset A)$.

Examiner la véracité de ces implications. Justifier les réponses à l'aide de diagrammes.

25. A est un ensemble de lettres; B est un ensemble de nombres entiers naturels. $A \times B$ contient 6 éléments.

Combien d'éléments peut-il y avoir dans A et B ?

Examiner complètement tous les cas; diagrammes.

26. Un ensemble $A \times B$ contient 7 éléments. Combien d'éléments peut-il y avoir dans A et B ?

27. Soient les ensembles

$$E = \{ a; b; c; d; e; f \}, \quad A = \{ a; c; d; f \}, \quad B = \{ c; d; e; f \}$$

1° Donner la liste des sous-ensembles de B.
2° Etudier $\mathcal{P}(A)$.
3° Quels sont les sous-ensembles de A qui sont aussi sous-ensembles de B ? Quels sont les sous-ensembles de B qui sont aussi sous-ensembles de A ?
Etudier :

$$[\mathcal{P}(A)] \cap [\mathcal{P}(B)].$$

4° Quels sont les sous-ensembles de B qui sont disjoints de A.
5° Étudier.

$$[\mathcal{P}(\complement A)] \cap [\mathcal{P}(\complement B)].$$

28. Quantifier les énoncés suivants :
1° Par tout point A il passe une droite D′ parallèle à une droite D quelconque donnée.
2° Par tout point A, il passe une droite D′ orthogonale à une droite D quelconque donnée.
3° Dans un triangle la somme des mesures des angles intérieurs est 180°.

29. Prendre la négation des assertions suivantes :

$(\forall x)$ (p et non q)	$(\forall x)$ (p ou non q)
$(\forall x)$ (non p et non q)	$(\forall x)$ (non p ou non q)
$(\exists x)$ (p et non q)	$(\exists x)$ (p ou non q)
$(\exists x)$ (non p et non q)	$(\exists x)$ (non p ou non q).

30. Soient les implications suivantes :

$$\text{non } p \Rightarrow q \qquad p \Rightarrow \text{non } q$$

1° Quelles sont les réciproques de ces implications.
2° Quelles sont les contraposées de ces deux implications.

31. Prendre les négations des trois assertions suivantes :
1° (p ou q) et q
2° ($p \Rightarrow q$) et r.
3° p ou ($q \Rightarrow r$).

32. Soient les ensembles :

$$A = \left\{ x/x \in N \quad \text{et} \quad x < \frac{13}{4} \right\}$$
$$B = \{ x/x \in N \quad \text{et} \quad x^2 \leqslant 25 \}$$

Énumérer les éléments de A et B.
Étudier le produit cartésien A × B.

33. Soient les ensembles :

$$A = \{ x/x \in R \quad \text{et} \quad 0 \leqslant x \leqslant 3 \}$$
$$B = \{ x/x \in R \quad \text{et} \quad -1 \leqslant x \leqslant 2 \}$$

Exprimer $A \cap B$ et $A \cup B$.

34. Résoudre les deux inéquations

$$2x^2 - 3x + 1 < 0$$

et

$$2x - 1 > 0.$$

Exprimer leurs solutions sous forme d'ensembles. Quelle est l'intersection de ces deux ensembles ?

Notion de correspondance.

35. On considère les deux ensembles A = { 1; 2; 3; 4; 5 } et B = { 1; 2; 3 }.
1° Soit la correspondance définie par

$$\begin{aligned} f: 3 &\longrightarrow 1 \\ 4 &\longrightarrow 2 \\ 5 &\longrightarrow 2 \\ 4 &\longrightarrow 3 \\ 1 &\longrightarrow 2. \end{aligned}$$

Donner le graphe de f. Quel est le diagramme de f? Quelle est la représentation graphique de f.

2° Déterminer la correspondance réciproque $\overset{-1}{f}$. Graphe et représentation graphique de $\overset{-1}{f}$.

36. Soit l'ensemble A = { 1; 2; 3; 4; 5; 6 }.

On considère la correspondance f de A dans A définie par :

$$\begin{aligned} f: 1 &\longrightarrow 2 \\ 2 &\longrightarrow 4 \\ 3 &\longrightarrow 3 \\ 4 &\longrightarrow 3 \\ 5 &\longrightarrow 3 \\ 6 &\longrightarrow 2. \end{aligned}$$

1° Diagramme de f.
2° Graphe et représentation graphique de f.

37. Soient les ensembles A = { 1; 2; 3; 4 } et B = { 1; 2; 3; 4; 5; 6 }.

On considère le graphe $G \subset A \times B$:

$$G = \{ (1;3); (2;5); (2;6); (3;1); (3;6); (4;5) \}$$

1° Donner le diagramme représentatif de G.
2° Montrer que G définit une correspondance f de A dans B.
3° Étudier la correspondance $\overset{-1}{f}$.

38. Soit l'ensemble A = { 1; 2; 3; 4; 5 }. Dans A × A, on donne le graphe G suivant :

$$G = \{ (1;1); (2;2); (3;3); (4;4); (5;5) \}.$$

Quelle est la nature de la correspondance f ainsi définie?

39. Soit l'ensemble A = { a; b; c; d; e }.

On envisage la correspondance f de A dans A définie par

$$\begin{aligned} f: a &\longrightarrow c \\ b &\longrightarrow d \\ c &\longrightarrow b \\ d &\longrightarrow a \\ e &\longrightarrow e. \end{aligned}$$

Quelle est la nature de f: application ou fonction? Quel est l'ensemble de définition; quel est l'ensemble des valeurs?

f est-elle injective, surjective, bijective?

40. Soient les ensembles $A = \{ a; b; c; d; e \}$ et $B = \{ 1; 2; 3; 4 \}$.

Soit f définie par :

$$\begin{aligned} f : b &\longrightarrow 2 \\ c &\longrightarrow 4 \\ d &\longrightarrow 1. \end{aligned}$$

1° f est-elle une fonction ou une application ? Quel est l'ensemble de départ ? Quel est l'ensemble de définition ?
2° f est-elle injective ?
3° Quel est l'ensemble d'arrivée ? Quel est l'ensemble des valeurs ? f est-elle surjective ?

41. Soient $A = \{ a; b; c; d \}$ et $B = \{ 1; 2; 3; 4 \}$
On considère f:

$$\begin{aligned} f : a &\longrightarrow 2 \\ b &\longrightarrow 3 \\ c &\longrightarrow 1 \\ d &\longrightarrow 4. \end{aligned}$$

1° Étude de f: diagramme; graphe; représentation graphique.
2° Déterminer A^* et B^*, f est-elle bijective ?

42. Soient $A = \{ a; b; c; d \}$ et $B = \{ 1; 2; 3; 4 \}$.

On envisage f:

$$\begin{aligned} f : a &\longrightarrow 2 \\ b &\longrightarrow 3 \\ c &\longrightarrow 1 \\ a &\longrightarrow 3. \end{aligned}$$

Étudier f.

43. Soit l'ensemble $E = \{ 1; 2; 3; 4; 5 \}$.
On définit f par

$$\begin{aligned} f: \text{ si } x < 2 &\longrightarrow f(x) = 3 \\ \text{si } x > 2 &\longrightarrow f(x) = 4 \\ \text{si } x = 2 &\longrightarrow f(x) = 1. \end{aligned}$$

1° Déterminer A^* et B^*.
2° Quelle est la nature de f? Diagramme de f.
3° Graphe et représentation graphique.
4° Etudier $\overset{-1}{f}$.

44. Soit dans N l'application f:

$$f : x \longrightarrow f(x) = x^2.$$

L'application f est injective, surjective ?

45. Dans $N = \{ 1; 2; 3; 4 \}$ on considère la fonction $f : x \longrightarrow x + 1$.
Quelle est la nature de f? Graphe. Représentation graphique.
f est-elle une surjection ?

46. On considère l'ensemble N, et la fonction $f: x \longrightarrow x$ de N dans N.
Nature de f. Graphe. Représentation graphique.

47. Soit l'ensemble $A = \{ 1; 2; 3; 4; 5 \}$.
On envisage la fonction f définie par :

$$\begin{aligned} f : x &\longrightarrow f(x) = x - 1 \quad \text{si} \quad x \neq 1 \\ x = 1 &\longrightarrow f(x) = 5 \end{aligned}$$

1° Étudier le graphe et la représentation graphique de f. Quelle est la nature de f?

2° Etudier $\overset{-1}{f}$.

48. Soit l'ensemble A = { 1; 2; 3; 4; 5; 6 }. On considère la fonction f?

$$f : x \in A \longrightarrow f(x) = \frac{6}{x} \in A.$$

1° Déterminer l'ensemble de définition A*.
2° Graphe, représentation graphique, nature de f.
3° Etudier la fonction $\overset{-1}{f}$.

49. Soit l'ensemble $E = \{ x/x \in N, \text{ et } 1 \leqslant x \leqslant 10 \}$. On envisage la fonction f définie de la façon suivante :

$$\begin{array}{llll} f : x \in E \longrightarrow f(x) = x & \text{si} & x \text{ est impair} \\ x \in E \longrightarrow f(x) = x - 1 & \text{si} & x \text{ est pair.} \end{array}$$

1° Déterminer A* et B*. Quelle est la nature de f?
2° Graphe et représentation graphique de f.
3° Etudier $\overset{-1}{f}$.

50. Soit l'ensemble E = { 1; 2; 3; 4 }. On envisage les deux permutations f et g de E :

$$f : \begin{array}{l} 2 \longrightarrow 1 \\ 3 \longrightarrow 4 \\ 4 \longrightarrow 3 \\ 1 \longrightarrow 2 \end{array} \qquad g : \begin{array}{l} 1 \longrightarrow 3 \\ 2 \longrightarrow 4 \\ 3 \longrightarrow 2 \\ 4 \longrightarrow 1. \end{array}$$

1° Graphes et représentations graphiques de f et g.
2° Etudier $g_o f$ et $f_o g$.
3° Etudier $\overset{-1}{f}_o \overset{-1}{g}$; $\overset{-1}{g}_o \overset{-1}{f}$; $(g_o f)^{-1}$; $(f_o g)^{-1}$.

51. Soit l'ensemble E = { a; b; c; d }. On considère les permutations suivantes de E :

$$f : \begin{array}{l} a \longrightarrow b \\ b \longrightarrow d \\ c \longrightarrow a \\ d \longrightarrow c \end{array} \qquad g : \begin{array}{l} a \longrightarrow d \\ b \longrightarrow c \\ c \longrightarrow b \\ d \longrightarrow a \end{array} \qquad h : \begin{array}{l} a \longrightarrow c \\ b \longrightarrow d \\ c \longrightarrow a \\ d \longrightarrow b. \end{array}$$

1° Déterminer $\overset{-1}{f}$; $\overset{-1}{g}$; $\overset{-1}{h}$.
2° Calculer $(h_o g)_o f$ et $h_o(g_o f)$. Remarque : Peut-on parler de $h_o g_o f$?
3° Calculer $\overset{-1}{f}_o \overset{-1}{g}_o \overset{-1}{h}$, puis $(h_o g_o h)_o (\overset{-1}{f}_o \overset{-1}{g}_o \overset{-1}{h})$.

52. Dans le plan P de la géométrie, on considère la relation d'orthogonalité entre droites.
1° Cette relation est-elle une relation binaire ?
2° Cette relation est-elle réflexive, symétrique, antisymétrique, transitive ?

53. Dans l'ensemble N des entiers naturels on considère la relation d'égalité-inégalité notée $\leqslant$.
Est-ce une relation binaire ? Quelles en sont les propriétés ?

54. Dans l'ensemble Z des nombres entiers rationnels (positifs, nul, négatifs) on considère la relation binaire $\mathcal{R}$ entre deux nombres quelconques a et b définie par

$$a \mathcal{R} b \iff a^2 + a = b^2 + b$$

Cette relation est-elle réflexive, symétrique, antisymétrique, transitive.

55. Dans le plan P de la géométrie on considère l'ensemble des cercles du plan.

1° On définit $\mathcal{R}$ par

$$(c)\mathcal{R}(c') \iff (c) \text{ et } (c') \text{ sont sécants : } (c) \cap (c') \neq \varnothing$$

Quelles sont les propriétés de cette relation binaire $\mathcal{R}$?

2° On définit $\mathcal{R}'$ par

$$(c)\mathcal{R}'(c') \iff (c) \cap (c') = \varnothing$$

Quelles sont les propriétés de la relation binaire R' ?

3° On définit $\mathcal{S}$ par

$$(c)\mathcal{S}(c') \iff (c) \text{ et } (c') \text{ ont le même centre.}$$

Quelles sont les propriétés de $\mathcal{S}$?

4° Reprendre les questions 1°, 2°, 3° en supposant que l'on considère deux disques Δ et Δ' au lieu des cercles (c) et (c').

56. Dans le produit cartésien R^2 on considère l'ensemble des homothéties, c'est-à dire l'ensemble des applications f telles que

$$f : (x\,;\,y) \in R^2 \longrightarrow f(x\,;\,y) = (kx\,;\,ky) = k(x\,;\,y) \quad \text{avec} \quad k \in R.$$

On définit une relation binaire $\mathcal{R}$ par

$$(x\,;\,y)\mathcal{R}(x'\,;\,y') \iff (\exists k) : (x'\,;\,y') = k\cdot(x\,;\,y).$$

Montrer que $\mathcal{R}$ est une relation d'équivalence. Quelles sont les classes d'équivalence ?

57. Dans l'ensemble N^2, on considère la relation binaire $\mathcal{R}$ définie par

$$(a\,;\,b)\mathcal{R}(a'\,;\,b') \iff a + b' = b + a'.$$

Montrer que $\mathcal{R}$ est une relation d'équivalence.

58. Dans l'ensemble Z^2, on considère la relation binaire $\mathcal{R}$:

$$(a\,;\,b)\mathcal{R}(a'\,;\,b') \iff ab' = ba'.$$

Est-ce une relation d'équivalence ?

59. Dans le plan P de la géométrie, on envisage une droite fixe Δ. Deux points M et N sont dits liés par la relation $\mathcal{R}$ si la droite MN est parallèle (au sens large) à la droite Δ.

La relation $\mathcal{R}$ est-elle une relation d'équivalence ?

Si oui, quelles sont les classes d'équivalence ?

60. Dans l'ensemble N on envisage la relation binaire $\mathcal{R}$ définie par

$$x\mathcal{R}y \iff x + y = 3.$$

Les couples (1; 2) (1; 1) (1; 4) (2; 1) (11; 14) appartiennent-ils au graphe de $\mathcal{R}$?

61. Soit l'ensemble E = { 1; 2; 3; 4; 5; 6 }.

Dans E on définit une relation binaire $\mathcal{R}$ par

$$x\mathcal{R}y \iff x - y = 1.$$

Donner le graphe de $\mathcal{R}$; et la représentation graphique de ce graphe.

62. Soit l'ensemble E = { 1; 2; 3; 4; 5; 6 }, on introduit la relation $\mathcal{R}$:

$$a\mathcal{R}b \iff a \leqslant b.$$

Donner le graphe de $\mathcal{R}$, et la représentation graphique de ce graphe.

63. Dans l'ensemble E = { 2; 3; 4; 5; 6; 8; 9; 12 }. On introduit dans E, la relation binaire notée | et définie par

$$(a \mid b) \iff (a \text{ divise } b).$$

1° Donner le graphe de cette relation ainsi que sa représentation graphique.

2° Montrer que cette relation est une relation d'ordre partiel sur E.

Cours Maintenon

64. Soit l'ensemble $E = \{ 1; 2; 3; 4; 5; 6 \}$. On considère le graphe G suivant de E^2 :

$$G = \{ (3;1); \quad (2;3); \quad (5;4); \quad (4;6); \quad (5;6); \quad (6;2) \}.$$

1° Représentation graphique de G. Quelles sont les projections de G?
2° Ce graphe G permet-il de définir une relation binaire $\mathcal{R}$?

65. Soit l'ensemble $E = \{ a; b; c; d; e \}$. On envisage le graphe G :

$$G = \{ (a;c); \quad (b;c); \quad (b;d); \quad (a;e) \}.$$

1° Quelle est la représentation graphique de G?
2° Quelle est la relation binaire $\mathcal{R}$ définie par G?

66. On considère l'ensemble $E = \{ 1; 2; 3; 4; 5; 6 \}$. On introduit dans E deux relations binaires $\mathcal{R}$ et $\mathcal{R}'$:

$$x \mathcal{R} y \iff x + 1 = y$$

et

$$x \mathcal{R}' y \iff x \leqslant y.$$

1° Graphe et représentation graphique de $\mathcal{R}$.
2° Graphe et représentation graphique de $\mathcal{R}'$.
3° On définit une nouvelle relation binaire $\mathcal{S}$ par

$$(x \mathcal{S} y) \iff (x \mathcal{R} y \text{ et } x \mathcal{R}' y)$$

Graphe et représentation graphique de $\mathcal{S}$.
4° On définit une quatrième relation binaire $\mathcal{S}'$ par

$$x \mathcal{S}' y \iff (x \mathcal{R} y \text{ ou } x \mathcal{R}' y)$$

Graphe et représentation graphique de $\mathcal{S}'$.

67. Soit $E = \{ 1; 2; 3; 4; 5; 6 \}$. On considère la relation $\mathcal{R}$ et la relation $\mathcal{R}'$ définies par :

$$x \mathcal{R} y \iff (x + 1 = y \text{ et } x \leqslant y)$$

et

$$x \mathcal{R}' y \iff (x + 1 = y \text{ ou } x \leqslant y)$$

Donner les graphes et les représentations graphiques de $\mathcal{R}$ et $\mathcal{R}'$.

68. Soit $E = \{ 1; 2; 3; 4; 5; 6; 7; 8; 9 \}$. On envisage les relations $\mathcal{R}$, $\mathcal{R}'$ et $\mathcal{S}$ définies par :

$$x \mathcal{R} y \iff y = x^2$$
$$x \mathcal{R}' y \iff y \leqslant 16 - x^2$$
$$\mathcal{S} = \mathcal{R} \text{ et } \mathcal{R}'$$

Donner les représentations graphiques de ces trois relations.

69. Soit l'ensemble $E = \{ 1; 2; 3; 4; 5 \}$, et dans E^2 on considère le graphe :

$$G = \{ (2;1); (1;4); (3;5); (4;2) \}.$$

1° Est-ce un graphe fonctionnel?
2° Montrer que G permet de définir une correspondance f. Préciser f.
3° Montrer que G permet de définir une relation binaire $\mathcal{R}$. Préciser $\mathcal{R}$.

70. Dans l'ensemble $E = \{ 1; 2; 3; 4; 5; 6; 7; 8 \}$ on introduit la relation $\mathcal{R}$ définie par

$$x \mathcal{R} y \iff x + 1 = y$$

1° Étudier le graphe et la représentation graphique de $\mathcal{R}$.
2° On considère dans E la relation binaire $\mathcal{S}$ définie par $\mathcal{S}$ = non $\mathcal{R}$. Étudier le graphe et la représentation graphique de $\mathcal{S}$.
Les relations $\mathcal{R}$ et $\mathcal{S}$ sont dites complémentaires. Justifier cette expression.

71. La relation binaire $\mathcal{R}$ est dite circulaire lorsque :

$$a\mathcal{R}b \quad \text{et} \quad b\mathcal{R}c \quad \Rightarrow \quad c\mathcal{R}a$$

Montrer qu'une relation réflexive et circulaire est une relation d'équivalence. Réciproque.

72. Dans Z on introduit la relation $\mathcal{R}$:

$$(a\mathcal{R}b) \quad \Leftrightarrow \quad (a - b \text{ est divisible par } 2).$$

Montrer qu'il s'agit d'une relation d'équivalence. Déterminer les classes.

73. On considère une partition d'un ensemble E. Montrer qu'on peut associer une relation d'équivalence à cette partition.

74. On considère un ensemble E muni d'un ordre partiel noté $\prec$. Une telle relation d'ordre peut se représenter par un diagramme de Hasse. Dans un tel diagramme un élément de E est représenté par un point; les points représentatifs de deux éléments comparables sont reliées par un segment non horizontal et si $a \prec b$ le point image de b est au dessus du point image de a.

La relation d'ordre envisagée ici est la relation de divisibilité :

$$(a \mid b) \quad \Leftrightarrow \quad (a \text{ divise } b)$$

1° Montrer que l'ensemble $E = \{ 1; 2; 4; 8 \}$ ordonné par cette relation a pour diagramme de Hasse celui de la figure Ex. 74 *a*.

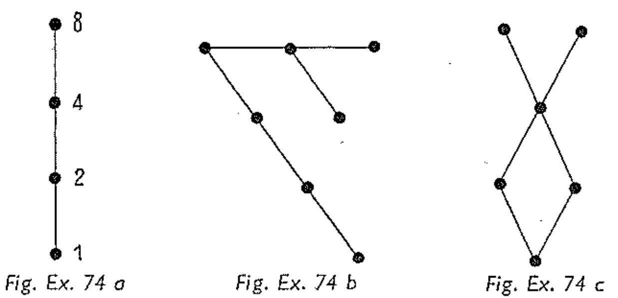


Fig. Ex. 74 a *Fig. Ex. 74 b* *Fig. Ex. 74 c*

2° Interpréter les diagrammes de Hasse des figures Ex. 74 *b* et Ex. 74 *c*.

75. Dans un ensemble E on envisage une relation $\mathcal{R}$ qui est supposée réflexive et transitive. On peut donc avoir $x\mathcal{R}y$ et $y\mathcal{R}x$ avec $y = x$.

On considère la relation $\mathcal{S}$ définie par

$$(x\mathcal{S}y) \quad \Leftrightarrow \quad (x\mathcal{R}y \quad \text{et} \quad y\mathcal{R}x)$$

1° Montrer que $\mathcal{S}$ est une relation d'équivalence.

2° Montrer que sur l'ensemble quotient $\frac{E}{\mathcal{S}}$ on peut définir un ordre naturellement associé à $\mathcal{R}$.

76. Un ensemble est dit bien ordonné si toute partie non vide admet un plus petit élément. Les ensembles suivants sont-ils bien ordonnés :

a) N, ensemble des entiers naturels

b) A, ensemble des rationnels compris entre 0 et 1 :

$$A = \{ x/x \in Q \quad \text{et} \quad 0 < x < 1 \}$$

c) $$B = \{ x/x \in Q \quad \text{et} \quad 0 \leqslant x \leqslant 1 \}$$

d) $$C = \left\{ \frac{1}{n} \middle/ n \in N^* \right\}; \quad N^* = N - \{ 0 \}$$

e) $$D = \left\{ 1 - \frac{1}{n} \middle/ n \in N^* \right\}.$$

SECONDE PARTIE

ALGÈBRE

LIVRE II

THÉORIE DES NOMBRES

CHAPITRE XI

LOIS DE COMPOSITION

87. Loi de composition interne.

1° ***Une loi de composition interne sur un ensemble E est une application f de E × E dans E, c'est-à-dire qu'à tout couple (x; y) ∈ E × E on fait correspondre un élément z de E.***

f: $$(x; y) \in E \times E \longrightarrow z = f(x; y) \in E.$$

L'image $f(x; y)$ du couple $(x; y)$ s'appelle le *composé de x et de y pour la loi donnée.*

Lorsque la fonction f est définie sur E × E, c'est-à-dire si $(E \times E)^* = E \times E$, on dit que *la loi est partout définie sur E.*

2° Au lieu de noter le composé z de $(x; y)$ par $z = f(x; y)$, on note de diverses façons suivant la loi utilisée.

*	e	a		y
e	e	a		
a	a	b		
x				x*y

Voici certaines notations employées :

$z = x + y$; lire « x plus y »
$z = x \cdot y$; lire « x multiplié par y »
$z = x * y$; lire « x astérisque y » ou « x étoile y » ou « x star y »
$z = x \top y$; lire « x truc y »
$z = x \perp y$; lire « x anti-truc y »

Cette liste de signes n'est évidemment pas limitative; et d'autres signes seront introduits par la suite.

Une loi notée + est dite loi notée additivement.

Une loi notée · est dite loi notée multiplicativement.

3° Une loi de composition interne est déterminée lorsqu'on connaît les images des couples de E × E.

Assez souvent on donne la loi à l'aide d'un tableau de composition qui se présente comme ci-dessus.

Dans la première colonne on place les éléments à gauche du signe $\ast$; dans la première ligne on place les éléments à droite du signe $\ast$.

Dans la case intersection de la ligne de x et de la colonne de y on place le composé $x \ast y$ de x et de y.

88. Partie stable.

Une partie A d'un ensemble E est dite stable pour la loi notée $\ast$ si le composé de deux éléments quelconques de A appartient à A.

Autrement dit :

$$(\text{A stable}) \Leftrightarrow [(\forall x)\ (\forall y)\ (x \in A \quad \text{et} \quad y \in A \Rightarrow x \ast y \in A)].$$

89. Loi associative.

1° ***Une loi de composition sur l'ensemble E, notée $\ast$, est associative si elle possède la propriété suivante :***

$$\boxed{A} \qquad (\forall x)\ (\forall y)\ (\forall z) : \quad (x \ast y) \ast z = x \ast (y \ast z)$$

$(x \ast y)$ représente le composé de x et de y; $(y \ast z)$ représente le composé de y et de z.

Si la loi notée $\ast$ est associative, on écrit :

$$(x \ast y) \ast z = x \ast (y \ast z) = x \ast y \ast z.$$

◇ *Exemple 1.*

L'addition et la multiplication dans l'ensemble N des nombres entiers naturels sont des lois de composition interne associatives :

$$(x + y) + z = x + (y + z)$$
$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

◇ *Exemple 2.*

Dans un ensemble totalement ordonné, par exemple dans N, les lois sup et inf (qui à deux nombres x et y font correspondre le plus grand, ou le plus petit, de ces deux nombres) sont associatives.

On a :

$$\sup [\sup (x; y); z] = \sup [x; \sup (y; z)]$$

car les deux membres désignent le plus grand des trois nombres x, y, z.

De même :

$$\inf [\inf (x; y); z] = \inf [x; \inf (y; z)]$$

◇ *Contre-exemple.*

Dans N la loi d'exponentiation n'est pas associative.
Si on note cette loi $\ast$, on a :

$$a \ast b = a^b.$$

Par suite :

$$(2 \ast 3) \ast 2 = 8 \ast 2$$
$$= 64$$
$$2 \ast (3 \ast 2) = 2 \ast 9$$
$$= 512$$

Donc :

$$(2 \ast 3) \ast 2 \neq 2 \ast (3 \ast 2)$$

ou

$$(2^3)^2 \neq 2^{(3^2)}.$$

La loi d'exponentiation n'est pas associative.

2° La loi notée $\ast$ étant associative on peut remplacer plusieurs éléments consécutifs par leur composé.

Ainsi, soit l'élément

$$A = \{ [(a_1 \ast a_2) \ast a_3] \ast a_4 \} \ast a_5.$$

On a (associativité dans l'accolade) :

$$A = \{ (a_1 \ast a_2) \ast (a_3 \ast a_4) \} \ast a_5$$
$$= (a_1 \ast a_2) \ast [(a_3 \ast a_4) \ast a_5]$$
$$= (a_1 \ast a_2) \ast (a_3 \ast a_4 \ast a_5).$$

On note alors :

$$A = a_1 \ast a_2 \ast a_3 \ast a_4 \ast a_5,$$

et éventuellement on peut faire réapparaître des parenthèses.

90. Eléments permutables. Lois commutatives.

1° ***Etant donnée une loi de composition, notée $\ast$, entre les éléments d'un ensemble E, deux éléments a et b sont dits permutables, ou échangeables, si a $\ast$ b et b $\ast$ a existent et si***

$$a \ast b = b \ast a,$$

On dit aussi que a et b commutent.

2° *Une loi de composition interne sur E est dite commutative si quels que soient les éléments x et y, ces éléments sont permutables.*

C'est donc une loi qui possède la propriété suivante :

$$\boxed{C} \qquad (\forall x)(\forall y) : \quad x * y = y * x.$$

◇ *Exemple 1.*

Dans N les lois d'addition et de multiplication sont commutatives :

$$x + y = y + x$$
$$x \cdot y = y \cdot x$$

◇ *Exemple 2.*

Dans l'ensemble N totalement ordonné les lois sup et inf sont commutatives :

$$\sup(x; y) = \sup(y; x)$$
$$\inf(x; y) = \inf(y; x)$$

◇ *Contre-exemple.*

La loi d'exponentiation dans N n'est pas commutative.

En effet :

$$2 * 3 = 8$$

et

$$3 * 2 = 9.$$

Donc :

$$2 * 3 \neq 3 * 2.$$

91. Loi associative et commutative.

1° Si la loi de composition interne notée $*$ est associative et commutative le composé de plusieurs éléments est indépendant de l'ordre de ces éléments et de leur groupement.

En effet, on peut permuter deux éléments consécutifs :

$$\begin{aligned} A &= a_1 * a_2 * a_3 * a_4 * a_5 \\ &= (a_1 * a_2) * (a_3 * a_4) * a_5 \\ &= (a_1 * a_2) * (a_4 * a_3) * a_5 \\ &= a_1 * a_2 * a_4 * a_3 * a_5. \end{aligned}$$

On peut ensuite, de la même façon, mettre les éléments dans un ordre assigné à l'avance.

2° On écrit :

$$x \mathrm{T} x = \overset{2}{\mathrm{T}} x$$

et plus généralement

$$\underbrace{x \top x \top \dots \top x}_{n \text{ éléments}} = \overset{n}{\top}\, x.$$

Lorsque la loi est notée additivement, on écrit :

$$\underbrace{x + x + \dots + x}_{n \text{ termes}} = nx$$

Si la loi est notée multiplicativement, on écrit :

$$\underbrace{x \cdot x \dots x}_{n \text{ facteurs}} = x^n.$$

92. Elément neutre.

***Un élément* e *de l'ensemble E est dit élément neutre pour la loi de composition sur E, notée* $*$, *si pour tout élément* x *de E, les éléments* e $*$ x *et* x $*$ e *existent, et sont égaux à* x.**

L'élément e est donc neutre pour la loi notée $*$ s'il possède la propriété suivante :

[N] $$(\exists e)\ (\forall x) \qquad x * e = e * x = x.$$

◇ *Exemple.*

Dans N, e = 0 est neutre pour l'addition car :

$$(\forall x) \qquad x + 0 = 0 + x = x$$

De même, dans N, ε = 1 est neutre pour la multiplication car :

$$(\forall x) \qquad 1 \times x = x \times 1 = x.$$

◇ *Contre-exemple.*

Pour l'exponentiation dans N, e = 0 n'est pas neutre, car :

$$0 * x = 0^x = 0$$

et

$$x * 0 = x^0 = 1.$$

ε = 1, non plus n'est pas neutre, car

$$1 * x = 1^x = 1$$

et

$$x * 1 = x^1 = x.$$

Remarque.

Le neutre d'une loi additive est noté 0 et s'appelle zéro.
Le neutre d'une loi multiplicative est noté 1 et s'appelle unité.

93. Eléments symétriques.

1° Soit une loi interne sur l'ensemble E, notée ✳ et possédant un élément neutre e.

Un élément a′ de E est dit symétrique de l'élément a de E relativement à la loi ✳ si on a

$$a \ast a' = a' \ast a = e.$$

On dit encore que a *est symétrisable (ou inversible) et qu'il admet* a′ *pour symétrique, relativement à la loi* ✳.

Si la loi est notée additivement, le symétrique a' de a pour l'addition est l'*opposé* de a, et on note $a' = -a$.

Si la loi est notée multiplicativement, le symétrique a' de a pour la multiplication est l'*inverse* de a, et on note $a' = a^{-1}$.

◇ *Exemple 1.*

Dans l'ensemble Z des entiers relatifs, $a = +2$ a pour opposé $a' = -2$, car :

$$a + a' = a' + a = 0.$$

◇ *Exemple 2.*

Dans l'ensemble Q des rationnels, $a = +\frac{2}{3}$ a pour opposé $a' = -\frac{2}{3}$, car :

$$a + a' = a' + a = 0;$$

mais $a = +\frac{2}{3}$ a pour inverse $a'' = +\frac{3}{2}$ car :

$$aa'' = a''a = 1.$$

2° ***Si tout élément de E a un symétrique, dans E, pour la loi ✳, on dit que E est symétrisé pour la loi ✳.***

Un ensemble symétrisé possède donc la propriété suivante :

[S] $$(\forall x)(\exists x') : \quad x \ast x' = x' \ast x = e.$$

◇ *Exemple.*

L'ensemble N n'est pas symétrisé pour l'addition.

L'ensemble Z est symétrisé pour l'addition, mais n'est pas symétrisé pour la multiplication.

L'ensemble Q est symétrisé pour l'addition, et $Q - \{0\}$ est aussi symétrisé pour la multiplication.

94. Eléments réguliers.

1° ***Un élément a de E est régulier à droite pour la loi $*$ s'il possède la propriété suivante :***

[Rd] $$(\forall x)\,(\forall y)\quad (x * a = y * a \Rightarrow x = y).$$

De même a est régulier à gauche s'il possède la propriété suivante :

[Rg] $$(\forall x)\,(\forall y)\quad (a * x = a * y \Rightarrow x = y).$$

2° ***Si un élément est régulier à droite et régulier à gauche, il est dit régulier ou simplifiable.***

Lorsqu'une loi est commutative tout élément régulier à droite (ou à gauche) est régulier.

◇ *Exemples.*

1° Dans N, tous les nombres sont réguliers à droite et à gauche pour l'addition; et :

$$a + x = a + y \Rightarrow x = y$$

et

$$x + a = y + a \Rightarrow x = y.$$

2° Dans $N^* = N - \{ 0 \}$ tous les éléments sont réguliers pour la multiplication; et :

$$a \neq 0 \qquad ax = ay \Rightarrow x = y$$
$$xa = ya \Rightarrow x = y.$$

95. Loi de composition externe.

Soient un ensemble Ω et un second ensemble E.

$\Omega = \{ \alpha; \beta; \gamma; ... \}$ est l'ensemble des opérateurs.

Au couple $(\alpha; x)$ formé d'un élément α de Ω et d'un élément x de E, on fait correspondre par une application f de $\Omega \times E$ dans E un élément $f(\alpha; x)$ de E.

L'élément $f(\alpha; x)$ s'appelle le composé de α et de x.

On note souvent

$$f(\alpha\,; x) = \alpha \,.\, x$$

◇ *Exemple.*

Si Ω est l'ensemble N des nombres entiers naturels et si $E = Q_+$ des nombres rationnels positifs, on définit une loi externe par :

$$f: \qquad (\alpha; x) \in N \times Q_+ \longrightarrow f(\alpha; x) = x^\alpha$$

C'est l'exponentiation entière dans Q.

96. Relations entre deux lois de composition interne. Distributivité.

1° ***Soit un ensemble E muni de deux lois internes notées*** $\top$ ***et*** $*$.

On dit que la loi $*$ ***est distributive à gauche pour la loi*** $\top$, ***si ces lois possèdent la propriété suivante :***

[DG] $(\forall x)(\forall y)(\forall z) : \quad x * (y \top z) = (x * y) \top (x * z).$

De même, la loi $*$ ***est distributive à droite pour la loi*** $\top$, ***si ces lois possèdent la propriété suivante :***

[DD] $(\forall x)(\forall y)(\forall z) : \quad (y \top z) * x = (y * x) \top (z * x).$

2° ***Si la loi*** $*$ ***est distributive à gauche et distributive à droite, elle est dite distributive.***

Si la loi $*$ est commutative, si de plus elle est distributive à gauche (ou à droite) elle est distributive.

◇ *Exemple.*

Dans N la multiplication est distributive pour l'addition; et :

$$x(y + z) = xy + xz$$
$$(y + z)x = yx + zx.$$

97. Relations entre une loi interne et une loi externe.

Soit la loi externe définie par :

$f: \qquad (\alpha; x) \in \Omega \times E \longrightarrow \alpha \cdot x \in E$

1° On suppose que l'ensemble E est muni d'une loi interne notée additivement.

La loi externe est dite distributive pour l'addition dans E, si les lois possèdent la propriété suivante :

[D′] $(\forall \alpha)(\forall x)(\forall y) \qquad \alpha(x + y) = \alpha x + \alpha y.$

2° On suppose que l'ensemble Ω est muni d'une loi interne notée additivement.

La loi externe est dite distributive pour l'addition dans Ω, ***si les lois possèdent la propriété suivante :***

[D″] $(\forall \alpha)(\forall \beta)(\forall x) \qquad (\alpha + \beta)x = \alpha x + \beta x.$

3° On suppose que l'ensemble Ω est muni d'une loi interne notée multiplicativement.

Il y a associativité mixte entre la loi externe et la multiplication dans Ω, si les lois possèdent la propriété suivante :

$\boxed{A'}$ $(\forall\alpha)\,(\forall\beta)\,(\forall x) \quad \alpha\cdot(\beta x) = (\alpha\beta)\,x.$

4° On suppose que l'ensemble E est muni d'une loi interne notée multiplicativement.

Il y a associativité mixte entre la loi externe et la multiplication dans E, si les lois possèdent la propriété suivante :

$\boxed{A''}$ $(\forall\alpha)\,(\forall x)\,(\forall y) \quad \alpha\cdot(xy) = (\alpha x)\cdot y = x\cdot(\alpha y).$

CHAPITRE XII

LES NOMBRES NATURELS

98. Ensembles équipotents.

Soient deux ensembles A et B.

L'ensemble A est équipotent à l'ensemble B s'il existe une application bijective de A sur B.

On note :

$$A \text{ eq } B \quad \text{ou} \quad \text{Eq}\,(A;\, B)$$

◇ *Exemple 1.*

Soient les ensembles :

$$A = \{\, a\,;\, b\,;\, c\,;\, d \,\}$$

et

$$B = \{\, \alpha;\, \beta;\, \gamma;\, \delta \,\}.$$

On envisage l'application f (fig. 98 *a*).

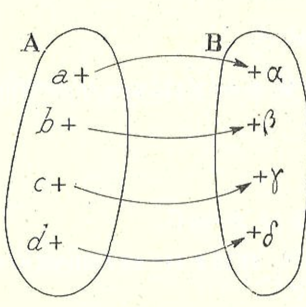


Fig. 98 a.

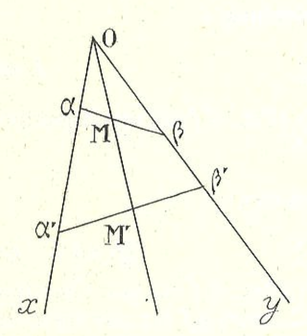


Fig. 98 b.

f :

$$a \longrightarrow f(a) = \alpha$$
$$b \longrightarrow f(b) = \beta$$
$$c \longrightarrow f(c) = \gamma$$
$$d \longrightarrow f(d) = \delta$$

f est une bijection de A sur B; donc les ensembles A et B sont équipotents.

◇ *Exemple 2.*

Soit un secteur angulaire $(Ox; Oy)$ (fig. 98 *b*). On considère deux points α et α' de Ox, et deux points β et β' de Oy.

On envisage les segments $\alpha\beta$ et $\alpha'\beta'$ en tant qu'ensembles de points.

$$A = (\alpha\beta)$$
$$B = (\alpha'\beta').$$

Soit l'application f qui à un point M de $A = (\alpha\beta)$ fait correspondre le point M' de $B = (\alpha'\beta')$, intersection de $\alpha'\beta'$ et de la droite OM. Cette application f est une bijection de A sur B; donc les ensembles A et B sont équipotents.

99. Cardinal d'un ensemble.

1° *L'équipotence est une relation d'équivalence.*

En effet, elle est :

réflexive :

[R] A eq A.

Il suffit de prendre comme bijection f l'identité e qui à l'élément x de A fait correspondre x;

symétrique :

[S] A eq B ⇒ B eq A.

En effet, si f est une bijection de A sur B, alors $\overset{-1}{f}$ est une bijection de B sur A;

transitive :

[T] (A eq B et B eq C) ⇒ A eq C.

En effet, si f est une bijection de A sur B, et si g est une bijection de B sur C, alors $g_\circ f$ est une bijection de A sur C.

2° *Cette relation d'équivalence partage les ensembles en classes d'équivalence.*

Une classe d'équivalence par équipotence d'un ensemble A est appelée la puissance de cet ensemble.

On dit aussi que c'est le *cardinal de l'ensemble A;* et on note :

Card (A)

Donc :

$$(A \text{ eq } B) \Leftrightarrow (\text{Card}(A) = \text{Card}(B))$$

Card (A) s'appelle encore un nombre.

◇ *Exemple 1.*

Les deux ensembles $A = \{a; b; c; d\}$ et $B = \{\alpha; \beta; \gamma; \delta\}$ de l'exemple 1 du numéro précédent sont équipotents et :

$$\text{Card}(A) = \text{Card}(B)$$

Les ensembles A et B ont le même nombre d'éléments; ici ce nombre est 4.

◇ *Exemple 2.*

Les deux ensembles de points $A = (\alpha\beta)$ et $B = (\alpha'\beta')$ de l'exemple 2 du numéro précédent sont équipotents et :

$$\text{Card}(A) = \text{Card}(B)$$

Les ensembles A et B ont le même nombre d'éléments; ici ce nombre est un nombre transfini noté $\mathfrak{C}$.

◇ *Exemple 3.*

Soient un segment $O\beta$ et son milieu α (fig. 99).

Fig 99.

On considère les ensembles de points constitués par les segments $O\alpha$ et $O\beta$:

$$A = (O\alpha) \quad \text{et} \quad B = (O\beta).$$

L'homothétie $\mathcal{H}(0; 2)$, de centre O et de rapport 2, est une bijection de A sur B; les deux ensembles A et B sont donc équipotents; et :

$$\text{Card}(A) = \text{Card}(B).$$

Les deux segments $A = (O\alpha)$ et $B = (O\beta)$ ont le même nombre de points; ce nombre est encore ici le nombre $\mathfrak{C}$.

100. Cardinal 0. Cardinal 1.

1° Le cardinal de l'ensemble vide est noté 0 :

$$\textbf{\textit{Card}}(\varnothing) = \mathbf{0}$$

2° Tous les ensembles à un élément sont équipotents. On note 1 le cardinal de ces ensembles :

$$Card(\{ a \}) = 1$$

101. Addition des cardinaux.

Soient deux ensembles disjoints A et B, $(A \cap B = \varnothing)$, avec

$$Card\ (A) = a \quad \text{et} \quad Card\ (B) = b$$

Par définition, le cardinal s de la réunion $A \cup B$ des deux ensembles est la somme de a et b.

Donc :

$$A \cap B = \varnothing : \quad \text{Card}\ (A \cup B) = \text{Card}\ (A) + \text{Card}\ (B)$$

ou

$$s = a + b.$$

◇ *Exemple 1.*

Soient les deux ensembles disjoints :

$$A = \{ a; b; c; d \} \quad \text{et} \quad B = \{ e; f \}$$

On a :

$$A \cup B = \{ a; b; c; d; e; f \}$$

et

$$\text{Card}\ (A \cup B) = \text{Card}\ (A) + \text{Card}\ (B).$$

Or :

$$\text{Card}\ (A \cup B) = 6, \quad \text{Card}\ (A) = 4, \quad \text{Card}\ (B) = 2.$$

Donc :

$$4 + 2 = 6.$$

◇ *Exemple 2.*

Soient le segment $O\beta$ et son milieu α (fig. 99).

On considère les ensembles de points suivants :

$$A = [O\alpha[, \quad B = [O\beta[, \quad C = [\alpha\beta[$$

constitués par les segments $(O\alpha)$, $(O\beta)$, $(\alpha\beta)$ privés respectivement des points α; β; β.

L'homothétie $\mathcal{H}(0; 2)$ est une bijection de A sur B; donc

$$\text{Card}\ (A) = \text{Card}\ (B).$$

La translation $\mathcal{T}(O\alpha)$ est une bijection de A sur C; donc

$$\text{Card}(A) = \text{Card}(C)$$

et finalement :

$$\text{Card}(A) = \text{Card}(B) = \text{Card}(C) = \mathfrak{C}.$$

Or : $B = A \cup C$ et $A \cap C = \varnothing$

et, par suite :

$$\text{Card}(B) = \text{Card}(A) + \text{Card}(C)$$

ou

$$\mathfrak{C} = \mathfrak{C} + \mathfrak{C}$$

102. Propriétés de l'addition des cardinaux.

L'addition des cardinaux possède les propriétés suivantes :

Commutativité.

Soient deux ensembles A et B disjoints, et leurs cardinaux a et b; on a :

$$A \cup B = B \cup A$$

D'où :

$$\text{Card}(A \cup B) = \text{Card}(B \cup A)$$

ou

$$\text{Card}(A) + \text{Card}(B) = \text{Card}(B) + \text{Card}(A)$$

c'est-à-dire :

$$a + b = b + a.$$

Associativité.

Soient trois ensembles A, B, C deux à deux disjoints, et leurs cardinaux a, b et c; on a :

$$(A \cup B) \cup C = A \cup (B \cup C).$$

D'où :

$$\text{Card}((A \cup B) \cup C) = \text{Card}(A \cup (B \cup C))$$

ou

$$\text{Card}(A \cup B) + \text{Card}\, C = \text{Card}\, A + \text{Card}(B \cup C)$$

c'est-à-dire :

$$(a + b) + c = a + (b + c).$$

Existence d'un élément neutre.

Soient l'ensemble A de cardinal a, et l'ensemble vide $\varnothing$ de cardinal 0. ($A \cap \varnothing = \varnothing$).

On a :

$$A \cup \varnothing = \varnothing \cup A = A.$$

D'où :

$$\text{Card}\,(A \cup \varnothing) = \text{Card}\,(\varnothing \cup A) = \text{Card}\,A$$

c'est-à-dire :

$$a + 0 = 0 + a = a.$$

103. Multiplication des cardinaux.

***Soient deux ensembles A et B, et leurs cardinaux* a *et* b.**
***Par définition, le cardinal* p *du produit cartésien A × B des deux ensembles est le produit de* a *et* b.**

Donc :

$$\text{Card}\,(A \times B) = \text{Card}\,(A) \cdot \text{Card}\,(B)$$

ou

$$p = a \cdot b.$$

◇ *Exemple.*

Soient les ensembles $A = \{ a; b; c \}$ et $B = \{ \alpha; \beta \}$, de cardinaux $a = 3$ et $b = 2$.

On a :

$$A \times B = \{ (a; \alpha); (a; \beta); (b; \alpha); (b; \beta); (c; \alpha); (c; \beta) \}$$

et

$$\text{Card}\,(A \times B) = \text{Card}\,(A) \cdot \text{Card}\,(B).$$

Or :

$$\text{Card}\,(A \times B) = 6, \quad \text{Card}\,(A) = a = 3, \quad \text{Card}\,(B) = b = 2.$$

Donc :

$$3 \times 2 = 6.$$

104. Propriétés de la multiplication des cardinaux.

La multiplication des cardinaux possède les propriétés suivantes :

Commutativité.

Soient les ensembles A et B, et les produits cartésiens $A \times B$ et $B \times A$. L'application f définie par

$$f : \qquad (x; y) \in A \times B \longrightarrow f(x; y) = (y; x) \in B \times A$$

est une bijection de A × B sur B × A. Donc :

$$(A \times B) \text{ eq } (B \times A)$$

et

$$\text{Card }(A \times B) = \text{Card }(B \times A)$$

ou

$$\text{Card }(A) \cdot \text{Card }(B) = \text{Card }(B) \cdot \text{Card }(A)$$

c'est-à-dire :

$$ab = ba.$$

Associativité.

Soient les ensembles A, B et C, et les produits cartésiens (A × B) × C et A × (B × C). L'application f définie par

$$f: \quad [(x;y);z] \in (A \times B) \times C \longrightarrow [x;(y;z)] \in A \times (B \times C)$$

est une bijection de (A × B) × C sur A × (B × C). Donc :

$$[(A \times B) \times C] \text{ eq } [A \times (B \times C)]$$

et

$$\text{Card }[(A \times B) \times C] = \text{Card }[A\ (B \times C)]$$

ou

$$\text{Card }(A \times B) \cdot \text{Card }(C) = \text{Card } A \times \text{Card }(B \times C)$$

c'est-à-dire :

$$(ab)c = a(bc).$$

Existence d'un élément neutre.

Soient l'ensemble A de cardinal a et l'ensemble $I = \{u\}$ formé du seul élément u.

L'application f définie par

$$f: \quad (x;u) \in A \times I \longrightarrow f(x;u) = x \in A$$

est une bijection de A × I sur A. Donc :

$$(A \times I) \text{ eq } A$$

et

$$\text{Card }(A \times I) = \text{Card }(A)$$

ou

$$\text{Card }(A) \cdot \text{Card }(I) = \text{Card }(A)$$

c'est-à-dire :

$$a \times 1 = a.$$

Par suite de la commutativité, on a :

$$a \times 1 = 1 \times a = a.$$

105. Distributivité de la multiplication pour l'addition.

Soient les ensembles A, B, C, avec $B \cap C = \varnothing$, et leurs cardinaux a, b, c.

On a :

$$A \times (B \cup C) = (A \times B) \cup (A \times C).$$

Donc :

$$\text{Card}\,[A \times (B \cup C)] = \text{Card}\,[(A \times B) \cup (A \times C)]$$

ou

$$\text{Card}\,(A) \times \text{Card}\,(B \cup C) = \text{Card}\,(A \times B) + \text{Card}\,(A \times C)$$

c'est-à-dire :

$$a\,(b + c) = ab + ac.$$

Ainsi la multiplication est distributive à gauche pour l'addition. La commutativité montre qu'il y a aussi distributivité à droite.

D'où :

La multiplication des cardinaux est distributive pour l'addition des cardinaux.

106. Multiplication par 0.

Si A est un ensemble quelconque on a :

$$A \times \varnothing = \varnothing.$$

Donc :

$$\text{Card}\,(A \times \varnothing) = \text{Card}\,(\varnothing)$$

c'est-à-dire :

$$\mathbf{a} \times 0 = 0.$$

107. Intégrité.

On sait que :

$$A \times B = \varnothing \Rightarrow (A = \varnothing \quad \text{ou} \quad B = \varnothing).$$

D'où :

$$\mathbf{ab} = 0 \Rightarrow (\mathbf{a} = 0 \quad \textit{ou} \quad \mathbf{b} = 0).$$

On traduit cette propriété en disant qu'il y a *intégrité*.

108. Cardinaux finis.

1° Soit un ensemble A de cardinal a.

***L'ensemble A est fini si son cardinal* a est tel que a ≠ a + *1*.**

Le cardinal d'un ensemble fini est dit fini.

***Un cardinal* a *est fini si* a $\neq$ a + *1*.**

2° *Il existe des cardinaux non finis.*

Ainsi le cardinal $\mathfrak{C}$ (cf. ex. 101) est un cardinal non fini car $\mathfrak{C} + \mathfrak{C} = \mathfrak{C}$.

3° *Il existe des cardinaux finis.*

Ainsi 0 est un cardinal fini; en effet de

$$0 \neq 1$$

on tire :

$$0 + 0 \neq 0 + 1$$

ou

$$0 \neq 0 + 1$$

et 0 est bien un cardinal fini.

4° *Les cardinaux finis constituent un ensemble noté* N :

$$N = \{ 0; \dots \}.$$

Les cardinaux finis sont aussi appelés les *nombres entiers naturels*

109. Propriété fondamentale des entiers naturels.

1° ***Lemme préliminaire.***

On se propose de démontrer l'implication

$$\mathbf{a} + \mathbf{1} = \mathbf{b} + \mathbf{1} \quad \Rightarrow \quad \mathbf{a} = \mathbf{b}.$$

Soit X un ensemble dont le cardinal est Card (X) $= a + 1 = b + 1$.

Il existe des parties A et $\{ u \}$ de X telles

$$X = A \cup \{ u \} \quad \text{et} \quad \complement_X A = \{ u \}$$

et des parties B et $\{ v \}$ de X telles que

$$X = B \cup \{ v \} \quad \text{et} \quad \complement_X B = \{ v \}$$

avec

$$\text{Card } A = a, \quad \text{Card } B = b,$$
$$\text{Card } (\{ u \}) = 1, \quad \text{Card } (\{ v \}) = 1.$$

Puisque $a + 1 = b + 1$, il existe une bijection f de $A' = A \cup \{ u \}$ sur $B' = B \cup \{ v \}$.

Fig. 109 *a*.

Si dans cette bijection u a pour image v, la restriction de f à A est une bijection de A sur B et par suite Card (A) = Card (B) ou $a = b$ (fig. 109 *a*).

Si dans cette bijection u a pour image l'élément $\alpha \neq v$, on envisage la permutation g de X qui échange α et v; $g_{o}f$ est une bijection de X sur X

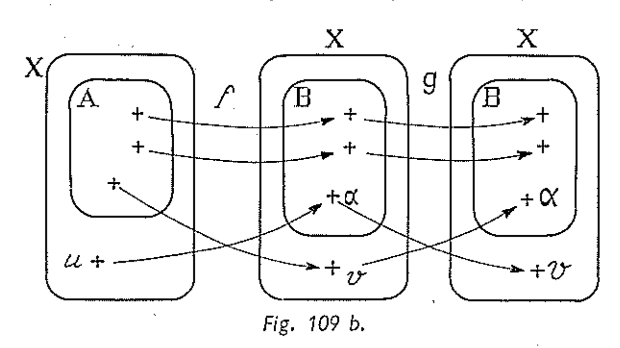


Fig. 109 b.

(fig. 109 *b*). La restriction de $g_{o}f$ à A est une bijection de A sur B; et par suite Card (A) = Card (B) ou $a = b$.

2° ***Propriété fondamentale.***

Cette propriété fondamentale s'énonce :

Si le nombre a est fini, alors le nombre a + 1 est fini.

C'est-à-dire :

$$\mathbf{a} \in \boldsymbol{N} \Rightarrow (\mathbf{a} + 1) \in \boldsymbol{N}.$$

Pour établir ce résultat on fait une réduction à l'absurde.

Si $a + 1$ n'était pas fini, on aurait $a + 1 = (a + 1) + 1$, d'après la définition des cardinaux finis; et d'après le lemme préliminaire, on déduirait de l'égalité précédente $a = a + 1$ et a ne serait pas fini, ce qui est contraire à l'hypothèse. Donc $a + 1$ est fini.

110. Récurrence.

1° *Axiome de récurrence.*

La propriété fondamentale précédente permet d'obtenir des nombres naturels par addition réitérée de 1.

On admet l'axiome suivant :

L'ensemble N se construit à partir de 0 par addition réitérée de 1.

Donc :

$$\mathrm{N} = \{0; 1; 2; \ldots\}$$

On pose :

$$\mathrm{N}^* = \mathrm{N} - \{0\}.$$

2° *Raisonnement par récurrence.*

On envisage une propriété P dépendant du nombre $n \in N$; cette propriété est notée $P(n)$.

Si la propriété P (0) est vraie et si quel que soit n, la propriété « P(n) vraie » implique la propriété « P(n + 1) vraie », alors, quel que soit n, la propriété P(n) est vraie.

Autrement dit :

$$\left.\begin{array}{l} P(0) \text{ vraie} \\ \text{et} \\ (\forall n) : P(n) \text{ vraie} \Rightarrow P(n+1) \text{ vraie} \end{array}\right\} \Rightarrow (\forall n) : P(n) \text{ vraie.}$$

En effet $P(0)$ étant vraie, $P(0 + 1) = P(1)$ est vraie; $P(1)$ étant vraie, $P(1 + 1) = P(2)$ est vraie; et ainsi de suite; donc $P(n)$ est vraie pour tous les entiers naturels.

3° *Remarque.*

Très souvent la récurrence commence à $P(1)$ ou $P(2)$ au lieu de $P(0)$.

111. Addition des entiers naturels.

La somme de deux cardinaux finis est un cardinal fini

ou

L'addition des cardinaux finis est une loi interne dans N.

Autrement dit :

$$(a \in N \quad \text{et} \quad b \in N) \Rightarrow a + b \in N.$$

On démontre ce résultat par une récurrence portant sur b.

Si $b = 0$, on a :

$$a + 0 = a$$

et la propriété est vraie pour $b = 0$; ou encore $P(0)$ est vraie.

Si $b = n$, on suppose que $P(n)$ est vraie, c'est-à-dire que $a + n \in N$. D'après la propriété fondamentale, on a :

$$a + n \in N \Rightarrow (a + n) + 1 \in N$$

et comme l'addition des cardinaux est associative on a :

$$a + (n + 1) \in N.$$

Autrement dit :

$$P(n) \text{ vraie} \Rightarrow P(n + 1) \text{ vraie.}$$

Donc par récurrence :

$$(\forall a)\,(\forall b)\,(a \in N \quad \text{et} \quad b \in N) \quad \Rightarrow \quad a + b \in N.$$

112. Propriétés de l'addition des entiers naturels.

Bien entendu comme pour les cardinaux, l'addition des entiers naturels possède les propriétés suivantes :

Commutativité.

C $$(\forall a)\ (\forall b) \quad a + b = b + a.$$

Associativité.

A $$(\forall a)\ (\forall b)\ (\forall c) \quad (a + b) + c = a + (b + c).$$

Existence d'un neutre.

N $$(\forall a) \quad a + 0 = 0 + a = a.$$

113. Régularité pour l'addition.

On se propose de démontrer que :

Tous les nombres naturels sont réguliers pour l'addition.

C'est-à-dire :

$$(\forall \mathbf{a})\ (\forall \mathbf{b})\ (\forall \mathbf{c}) : \quad \mathbf{a + c = b + c \Rightarrow a = b}.$$

Ce résultat se démontre par une récurrence portant sur c.

Si $c = 1$, d'après le lemme préliminaire on a :

$$a + 1 = b + 1 \Rightarrow a = b.$$

Autrement dit $P(1)$ est vraie.

Si $c = n$, on suppose que $P(n)$ est vraie, c'est-à-dire que :

$$a + n = b + n \Rightarrow a = b.$$

Or si on a :

$$a + (n + 1) = b + (n + 1)$$

on déduit (associativité) :

$$(a + n) + 1 = (b + n) + 1.$$

D'où d'après le lemme préliminaire,

$$a + n = b + n$$

et, d'après l'hypothèse posée,

$$a = b.$$

Ainsi :

$$P(n) \text{ vraie} \Rightarrow P(n+1) \text{ vraie}.$$

Donc par récurrence :

$$(\forall a)\ (\forall b)\ (\forall c) : \quad a + c = b + c \Rightarrow a = b.$$

114. Somme nulle.

Soient deux ensembles, finis et disjoints, A et B, et leurs cardinaux a et b. On a :

$$a + b = 0 \Rightarrow A \cup B = \varnothing \Rightarrow (A = \varnothing \text{ et } B = \varnothing) \Rightarrow (a = 0 \text{ et } b = 0).$$

Donc :

Si la somme de deux nombres naturels est nulle, alors ces deux nombres sont nuls.

Et :

$$\mathbf{a} + \mathbf{b} = 0 \Rightarrow \mathbf{a} = \mathbf{b} = 0.$$

115. Ordre sur l'ensemble N.

1° ***On dit que*** **a** ***est inférieur ou égal à*** **b*****, s'il existe un nombre entier naturel*** **c** ***tel que*** $\mathbf{b} = \mathbf{a} + \mathbf{c}$.

On a :

$$(a \leqslant b) \Rightarrow [(\exists c) : b = a + c].$$

L'inégalité envisagée ici, notée $\leqslant$, est dite *inégalité large*. Si l'égalité est exclue, on note $<$, et l'*inégalité est stricte*.

2° *Cette relation entre nombres entiers naturels est une relation d'ordre* car elle possède les propriétés suivantes :

Réflexivité.

R $\qquad (\forall a) \quad a \leqslant a.$

En effet :

$$a \leqslant a + 0.$$

Antisymétrie.

AS $\qquad (\forall a)\ (\forall b) \quad (a \leqslant b \text{ et } b \leqslant a) \Rightarrow (a = b).$

En effet :

$$a \leqslant b \Rightarrow (\exists c) : \quad b = a + c$$

et

$$b \leqslant a \Rightarrow (\exists d) : \quad a = b + d.$$

On en déduit :

$$\begin{aligned} b &= a + c \\ &= b + d + c \end{aligned}$$

c'est-à-dire, d'après la régularité :

$$0 = c + d$$

ce qui implique (cf. nº 114) :

$$c = d = 0$$

ou finalement $\quad a = b.$

Transitivité.

$\boxed{T}$ $\quad (\forall a)\ (\forall b)\ (\forall c) : \quad (a \leqslant b \quad \text{et} \quad b \leqslant c) \Rightarrow (a \leqslant c).$

En effet : $\quad a \leqslant b \Rightarrow (\exists d) : \quad b = a + d$

et $\quad b \leqslant c \Rightarrow (\exists d') : \quad c = b + d'.$

D'où : $\quad b + c = a + b + d + d'$

ou $\quad c = a + (d + d')$

c'est-à-dire : $\quad a \leqslant c.$

116. L'ordre sur N est total.

On se propose de montrer que, quels que soient les nombres naturels a *et* b, *on a* a $\leqslant$ b *ou* b $\leqslant$ a.

Pour cela on fait une récurrence portant sur b.

Si $b = 0$, on a $0 \leqslant a$; puisque $a = a + 0$. Autrement dit P(0) est vraie.

Si $b = n$, on suppose que P(n) est vraie; c'est-à-dire que $a \leqslant n$ ou $n \leqslant a$.

On a :

$$(a \leqslant n \quad \text{ou} \quad n < a) \Rightarrow (a \leqslant n + 1 \quad \text{ou} \quad n + 1 \leqslant a).$$

Autrement dit :

$$\text{P}(n) \text{ vraie} \Rightarrow \text{P}(n + 1) \text{ vraie}.$$

Donc, par récurrence

$$(\forall a)(\forall b) : \quad (a \leqslant b \quad \text{ou} \quad b \leqslant a)$$

et :

L'ordre sur N, noté $\leqslant$, est un ordre total.

117. Addition et ordre.

Soient deux nombres entiers naturels a et b tels que $a \leqslant b$.

On a :

$$(a \leqslant b) \Rightarrow [(\exists d) : b = a + d] \Rightarrow [b + c = (a + c) + d] \Rightarrow a + c \leqslant b + c.$$

Donc :

$$(\forall c) \ (a \leqslant b) \Rightarrow a + c \leqslant b + c.$$

Et :

L'ordre total sur N est compatible avec l'addition.

118. Soustraction.

Soient deux nombres entiers naturels a et b avec $a \geqslant b$.

On a :

$$(a \geqslant b) \Rightarrow (\exists d) : \quad a = b + d.$$

Le nombre d *est la différence entre le nombre* a *et le nombre* b.

On note :

$$d = a - b.$$

119. Multiplication des entiers naturels.

Le produit de deux cardinaux finis est un cardinal fini.

ou

La multiplication des cardinaux finis est une loi interne dans N.

Autrement dit :

$$(\mathbf{a} \in N \quad \text{et} \quad \mathbf{b} \in N) \Rightarrow \mathbf{ab} \in N.$$

On démontre ce résultat par une récurrence portant sur b.

Si $b = 0$, on a :

$$a \cdot 0 = 0;$$

et la propriété est vraie pour $b = 0$; ou encore $P(0)$ est vraie.

Si $b = n$, on suppose que $P(n)$ est vraie, c'est-à-dire que $an \in N$.

On a, par suite de la distributivité (cf. 105) :

$$a(n+1) = an + a.$$

Or an et a appartiennent à N; il en est donc de même de

$$an + a = a(n+1).$$

Autrement dit :

$$P(n) \text{ vraie} \Rightarrow P(n+1) \text{ vraie}.$$

Donc, par récurrence :

$$(\forall a)\,(\forall b) \quad (a \in N \quad \text{et} \quad b \in N) \Rightarrow ab \in N.$$

120. Propriétés de la multiplication des entiers naturels.

Bien entendu comme pour les cardinaux, la multiplication des entiers naturels possède les propriétés suivantes :

Commutativité.

[C] $\qquad (\forall a)\,(\forall b) : \quad ab = ba.$

Associativité.

[A] $\qquad (\forall a)\,(\forall b)\,(\forall c) : \quad (ab)\,c = a\,(bc).$

Existence d'un neutre.

[N] $\qquad (\forall a) : \quad a \cdot 1 = 1 \cdot a = a.$

Distributivité de la multiplication pour l'addition.

[Dg] $\qquad (\forall a)\,(\forall b)\,(\forall c) \quad a\,(b + c) = ab + ac$

[Dd] $\qquad (\forall a)\,(\forall b)\,(\forall c) \quad (b + c)\,a = ba + ca.$

121. Régularité pour la multiplication.

On se propose de démontrer que tous les nombres naturels, *sauf* 0, sont réguliers pour la multiplication, c'est-à-dire que

$$(\forall \mathbf{a})\,(\forall \mathbf{b})\,(\forall \mathbf{c}) : \quad (\mathbf{c} \neq 0 \quad \textbf{et} \quad \mathbf{ac} = \mathbf{bc}) \Rightarrow (\mathbf{a} = \mathbf{b}).$$

En effet :

$$ac = bc \Rightarrow ac - bc = 0 \Rightarrow c\,(a - b) = 0.$$

D'après l'intégrité (cf. nº 107), $c\,(a-b) = 0$ entraîne $a - b = 0$ puisque c n'est pas nul, c'est-à-dire finalement $a = b$.

Donc :

Tous les nombres de $N^* = N - \{0\}$ sont réguliers pour la multiplication.

122. Multiplication et ordre.

Soient deux nombres entiers naturels a et b, avec $a \leqslant b$, et un troisième nombre entier naturel c.

On a :

$$(a \leqslant b) \Rightarrow [(\exists d) : b = a + d].$$

D'où :

$$bc = (a + d) \cdot c$$
$$= ac + cd.$$

Donc :

$$(\forall c)\ (\exists d) : \quad bc = ac + cd.$$

Par suite :

$$ac \leqslant bc.$$

Et finalement :

$$(\forall c) \quad (a \leqslant b) \Rightarrow ac \leqslant bc.$$

Et :

L'ordre total sur N est compatible avec la multiplication.

123. Multiples d'un nombre naturel. Exponentiation.

Soit un nombre entier naturel a, non nul.

Les produits

$$a \quad 2a \quad 3a \dots na \dots$$

sont les *multiples* de a.

1º Soit un nombre $a \cdot (a \in N)$.

Le produit de n ($n \in N$) facteurs égaux au nombre a est un nombre entier appelé puissance n^ième^ de a.

On note :

$$\mathbf{a}^n = \underbrace{\mathbf{a} \cdot \mathbf{a} \cdot \ldots \cdot \mathbf{a}}_{\mathbf{n}\ \textit{facteurs}}$$

n est *l'exposant de la puissance;* et a^n se lit « *a* puissance *n* » ou « *a* exposant *n* ».

2° On a :

$$a^n \cdot a^p = \underbrace{a \cdot a \ldots a}_{n \text{ facteurs}} \underbrace{a \cdot a \ldots a}_{p \text{ facteurs}}$$

$$= \underbrace{a \cdot a \ldots a}_{n + p \text{ facteurs}}.$$

D'où la formule :

$$\mathbf{a}^n \cdot \mathbf{a}^p = \mathbf{a}^{n+p}.$$

3° On a :

$$(a^n)^p = \underbrace{a^n \cdot a^n \ldots a^n}_{p \text{ facteurs}}$$

$$= a^{n+n+\cdots+n}$$

$$= a^{np}.$$

D'où la formule :

$$(\mathbf{a}^n)^p = \mathbf{a}^{np}.$$

124. Ensembles dénombrables.

1° L'ensemble des nombres de N n'est pas fini.

Le cardinal de l'ensemble N est un nombre non fini appelé « aleph zéro ». On le note :

$$\textit{Card}\,(N) = \aleph^0$$

2° Un ensemble équipotent à N est dit *ensemble dénombrable.*

Donc :

Pour qu'un ensemble E soit dénombrable il faut et il suffit qu'il existe une bijection de N sur E.

◇ *Exemple.*

Soit P l'ensemble de tous les nombres pairs :

$$P = \{\ 0;\ 2;\ 4;\ \ldots;\ 2\,n;\ \ldots\ \}.$$

On peut envisager l'application f de N sur P définie par

$$f: \quad \begin{array}{l} 0 \in N \longrightarrow 0 \in P \\ 1 \in N \longrightarrow 2 \in P \\ 2 \in N \longrightarrow 4 \in P \\ \ldots\ldots\ldots\ldots\ldots \\ n \in N \longrightarrow 2n \in P \\ \ldots\ldots\ldots\ldots\ldots \end{array}$$

est bien une bijection de N sur P. Donc :

$$\text{Card}(P) = \text{Card}(N) = \aleph_0.$$

3° ***L'ensemble N² est dénombrable.***

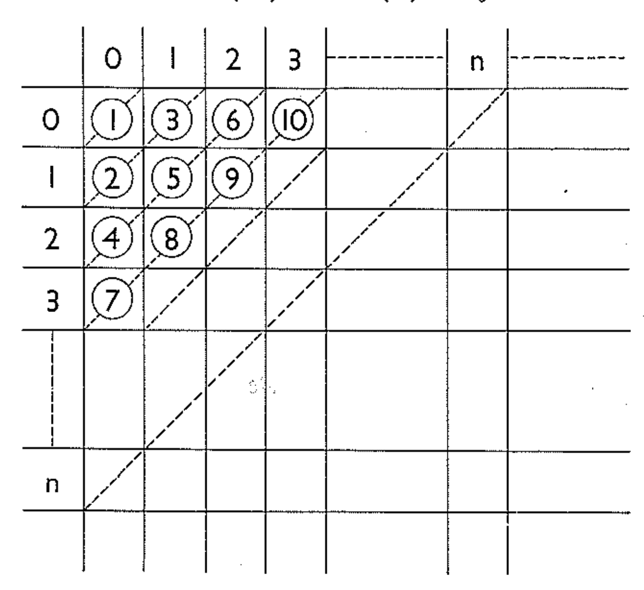
Le produit cartésien $N^2 = N \times N$ peut être représenté par le tableau à double entrée suivant :

	0	1	2	3	----------	n	----------
0	(0;0)	(1;0)	(2;0)	(3;0)	----------	(n;0)	----------
1	(0;1)	(1;1)	(2;1)	(3;1)	----------	(n;1)	----------
2	(0;2)	(1;2)	(2;2)	(3;2)	----------	(n;2)	----------
3	(0;3)	(1;3)	(2;3)	(3;3)	----------	(n;3)	----------
⋮	----	----	----	----	----------	----	----------
n	(0;n)	(1;n)	(2;n)	(3;n)	----------	(n;n)	----------
----	----	----	----	----	----------	----	----------

On établit une bijection entre N et les cases du tableau, c'est-à-dire entre N et N^2, en « numérotant » les cases suivant les diagonales montantes, conformément au tableau suivant :

On a donc :

$$\text{Card}\,(N^2) = \text{Card}\,(N) = \aleph_0$$



Plus généralement si n est un nombre naturel fini :

$$\text{Card}\,(N^n) = \text{Card}\,(N) = \aleph_0$$

125. Suites finies. Suites dénombrables.

1° *Suites à un indice.*

Soit un ensemble E d'éléments. On considère une application f de N dans E.

L'image de n par f est désignée par $f(n)$ ou encore par f_n (notation indicielle).

Les images.

$$f(0),\quad f(1),\quad f(2)\quad \dots\quad f(n)\quad \dots$$

ou

$$f_0\quad f_1\quad f_2\quad \dots\quad f_n\quad \dots$$

dans l'ordre indiqué constituent une *suite infinie dénombrable à un indice.*

Assez souvent on considère au lieu de N l'ensemble fini

$$I = \{\ 1; 2; \dots; n\ \}.$$

La suite

$$f_1\ f_2\ \dots\ f_n$$

est alors une *suite finie à un indice.*

◇ *Exemple 1.*

Soit l'ensemble E = { a; b; c; d; e }. On peut envisager l'application f de I = { 1; 2; 3; 4; 5 } sur E définie par

f :

$$\begin{aligned} 1 &\longrightarrow f_1 = a \\ 2 &\longrightarrow f_2 = c \\ 3 &\longrightarrow f_3 = d \\ 4 &\longrightarrow f_4 = b \\ 5 &\longrightarrow f_5 = e \end{aligned}$$

Alors :

$$a; c; d; b; e$$

est une suite finie de 5 éléments.

◇ *Exemple 2.*

Soient l'ensemble E = { a; b; c; d; e } et l'ensemble

I = { 1; 2; 3; 4; 5; 6; 7 }.

On envisage l'application u de I dans E définie par

u :

$$\begin{aligned} 1 &\longrightarrow u_1 = a \\ 2 &\longrightarrow u_2 = b \\ 3 &\longrightarrow u_3 = c \\ 4 &\longrightarrow u_4 = c \\ 5 &\longrightarrow u_5 = a \\ 6 &\longrightarrow u_6 = b \\ 7 &\longrightarrow u_7 = a. \end{aligned}$$

Alors :

$$(u_1 = a;\ u_2 = b;\ u_3 = c;\ u_4 = c;\ u_5 = a;\ u_6 = b;\ u_7 = a)$$

est une suite finie, de 7 éléments, à un indice.

◇ *Exemple 3.*

Soit l'application u de N dans N définie par

u :

$$\begin{aligned} 0 &\longrightarrow u_0 = 0 \\ 1 &\longrightarrow u_1 = 2 \\ 2 &\longrightarrow u_2 = 4 \\ 3 &\longrightarrow u_3 = 6 \\ &\cdots\cdots\cdots \\ n &\longrightarrow u_n = 2n \\ &\cdots\cdots\cdots \end{aligned}$$

La suite ainsi obtenue :

$$0 \quad 2 \quad 4 \quad 6 \quad \ldots \quad 2n \quad \ldots$$

est la suite infinie à un indice des nombres pairs.

2° ***Suites à deux indices.***

Soit un ensemble E d'éléments. On considère une application f de N^2 dans E. L'image de $(n;\ p) \in N^2$ est désignée par $f(n;\ p)$ ou encore par $f_{(n;\ p)}$ (notation indicielle).

Les images peuvent être placées en tableau (analogue à celui du n° 124)

$$\begin{array}{cccccccc} f_{(0;0)} & f_{(1;0)} & f_{(2;0)} & f_{(3;0)} & \cdots & f_{(n;0)} & \cdots \\ f_{(0;1)} & f_{(1;1)} & f_{(2;1)} & f_{(3;1)} & \cdots & f_{(n;1)} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ f_{(0;n)} & f_{(1;n)} & f_{(2;n)} & f_{(3;n)} & \cdots & f_{(n;n)} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{array}$$

Ces images constituent une *suite infinie dénombrable à deux indices. Le premier indice correspond à la colonne; le second indice correspond à la ligne.*

Assez souvent on considère au lieu de N^2 le produit cartésien $I \times J$ avec $I = \{\ 1;\ 2;\ \ldots;\ n\ \}$ et $J = \{\ 1;\ 2;\ \ldots;\ p\ \}$.

La suite obtenue placée en tableau est :

$$\begin{array}{ccccc} f_{(1;1)} & f_{(2;1)} & f_{(3;1)} & \cdots & f_{(n;1)} \\ f_{(1;2)} & f_{(2;2)} & f_{(3;2)} & \cdots & f_{(n;2)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ f_{(1;p)} & f_{(2;p)} & f_{(3;p)} & \cdots & f_{(n;p)} \end{array}$$

◇ *Exemple 1.*

On considère l'application f de N^2 dans N définie par

$$f: \qquad (n;p) \longrightarrow f\,(n;p) = f_{(n;p)} = n\,2^p.$$

La suite est alors :

$$\begin{array}{lllll} f_{(0;0)} = 0 & f_{(1;0)} = 1 & \ldots\ f_{(n;0)} = n & \ldots \\ f_{(0;1)} = 0 & f_{(1;1)} = 2 & \ldots\ f_{(n;1)} = 2n & \ldots \\ \cdots & \cdots & \cdots & \cdots \\ f_{(0;p)} = 0 & f_{(1;p)} = 2^p & \ldots\ f_{(n;p)} = n \cdot 2^p & \ldots \\ \cdots & \cdots & \cdots & \cdots \end{array}$$

C'est une suite infinie dénombrable à deux indices.

◇ *Exemple* 2.

On considère l'application u de $I \times J$ dans N, avec

$$I = \{ 1; 2; 3; 4 \} \quad \text{et} \quad J = \{ 1; 2 \}$$

définie par

u : $$(i;j) \in I \times J \longrightarrow u_{i;j} = i^i \times j^2$$

La suite est alors :

$u_{1;1} = 1$ $u_{2;1} = 4$ $u_{3;1} = 27$ $u_{4;1} = 256$ $u_{5;1} = 3125$

$u_{1;2} = 4$ $u_{2;2} = 16$ $u_{3;2} = 108$ $u_{4;2} = 1024$ $u_{5;2} = 12500$

C'est une suite finie à deux indices.

126. Division euclidienne.

1° ***Soient* a *et* b *deux entiers naturels avec* b $\neq$ *0.***
Il existe deux entiers* q *et* r *tels que

$$\mathbf{a = bq + r \quad et \quad r < b}$$

et les entiers* q *et* r *sont déterminés de façon unique par ces conditions.

Pour démontrer ce théorème, on considère la suite des multiples de b :

$$0 \quad b \quad 2b \quad \dots \quad bq \quad b(q+1) \quad \dots$$

Si le nombre a *appartient à cette suite*, on a :

$$a = bq; \qquad (126; 1)$$

q est déterminé de façon unique, et $r = 0$.

Si le nombre a *n'appartient pas à la suite*, il est compris entre deux éléments de la suite, et on a :

$$bq < a < b\,(q+1) \qquad (126; 2)$$

est déterminé de façon unique; et on a

$$0 < a - bq < b$$

$r = a - bq$ est alors déterminé de façon unique.

Les deux relations (126; 1) et (126; 2) se réunissent sous la formule

$$bq \leqslant a < b\,(q+1).$$

2° ***Diviser a par b, c'est déterminer les nombres q et r.***

Le nombre q est le *quotient entier de* a *par* b; le nombre r est le *reste de la division* de a par b.

3° Si $r = 0$, a est un multiple de b; on dit alors que b *est un diviseur* de a.

127. Développement de base *b*.

Un nombre a peut s'écrire de façon unique sous la forme

$$\mathbf{a} = \alpha_n \mathbf{b}^n + \alpha_{n-1}\mathbf{b}^{n-1} + \ \dots \ + \alpha_1 \cdot \mathbf{b} + \alpha_0,$$

Les nombres α_0; α_1; α_2; ...; α_n étant inférieurs à b. Ce sont des *chiffres*. *On dit qu'on a développé* a *suivant la base* b.

On note :

$$a = \overline{\alpha_n \alpha_{n-1} \ \dots \ \alpha_1 \alpha_0}$$

et le nombre est exprimé dans la base b.

128. Remarques.

1° *La notation* Inf (a; b) *désigne le plus petit des deux nombres* a et b; c'est-à-dire que :

$$\mathbf{Inf\,(a;\,b) = a} \quad \textit{si} \quad \mathbf{a \leqslant b}$$

et

$$\mathbf{Inf\,(a;\,b) = b} \quad \textit{si} \quad \mathbf{b \leqslant a.}$$

La notation Sup (a; b) *désigne le plus grand des deux nombres* a et b; c'est-à-dire que :

$$\mathbf{Sup\,(a;\,b) = b} \quad \textit{si} \quad \mathbf{a \leqslant b}$$

et

$$\mathbf{Sup\,(a;\,b) = a} \quad \textit{si} \quad \mathbf{b \leqslant a.}$$

2° On a la formule :

$$\mathbf{k + Inf\,(a;\,b) = Inf\,(k + a;\,k + b).}$$

En effet :

Si $a \leqslant b$, $\mathrm{Inf}\,(a;\ b) = a$; et $k + a \leqslant k + b$ entraîne :

$$\mathrm{Inf}\,(k + a;\ k + b) = k + a;$$

donc on a bien : $k + \mathrm{Inf}\,(a;\ b) = \mathrm{Inf}\,(k + a;\ k + b)$.

Si $b \leqslant a$, $\mathrm{Inf}\,(a;\ b) = b$; et $k + b \leqslant k + a$ entraîne :

$$\mathrm{Inf}\,(k + a;\ k + b) = k + b;$$

donc on a bien : $k + \mathrm{Inf}\,(a;\ b) = \mathrm{Inf}\,(k + a;\ k + b)$.

3º On démontre de même la formule :

$$\mathbf{k + Sup\ (a; b) = Sup\ (k + a; k + b).}$$

4º On a la formule :

$$\mathbf{a + b = Inf\ (a; b) + Sup\ (a; b).}$$

En effet :

Si $a \leqslant b$, $\text{Inf}\ (a; b) = a$ et $\text{Sup}\ (a; b) = b$ et on a bien :

$$\text{Inf}\ (a;\ b) + \text{Sup}\ (a;\ b) = a + b;$$

Si $b \leqslant a$, $\text{Inf}\ (a; b) = b$ et $\text{Sup}\ (a; b) = a$ et on a bien :

$$\text{Inf}\ (a; b) + \text{Sup}\ (a; b) = a + b.$$

5º On démontre de même la formule :

$$\mathbf{ab = Inf\ (a; b) \cdot Sup\ (a; b).}$$

CHAPITRE XIII

ANALYSE COMBINATOIRE

129. Arrangements.

Soient l'ensemble I = { 1; 2; ...; p } et un ensemble E de n éléments distincts (n ⩾ p). On considère une injection de I dans E. L'image de I est une suite finie de p éléments distincts de E.

Une telle suite est appelée un arrangement de p éléments pris parmi les n éléments de E.

On se propose ici de dénombrer le nombre des injections de I dans E, c'est-à-dire le nombre des arrangements de n éléments distincts p à p.

On peut choisir comme image de 1 l'un quelconque des n éléments de E. Il y a donc n possibilités de choisir cette image.

L'image de 1 étant choisie, on peut choisir l'image de 2 parmi les $n-1$ éléments restants; il y a $n(n-1)$ possibilités de choisir les images de 1, 2. De même, il y a $n(n-1)(n-2)$ possibilités de choisir les images de 1, 2 et 3.

Et ainsi de suite....

Il y a alors $n(n-1) \dots (n-p+1)$ possibilités de choisir les images de $\{ 1; 2; \dots; p \}$.

Ainsi :

Il y a $n(n-1) \dots (n-p+1)$ injections de I dans E;
ou $n(n-1) \dots (n-p+1)$ suites de p éléments pris parmi les n éléments de E;
ou $n(n-1) \dots (n-p+1)$ arrangements de n éléments distincts p à p.

On note :

$$A_n^p = n(n-1) \ \dots \ (n-p+1).$$

En posant (1)

$$n! = 1 \cdot 2 \cdot 3 \ \dots \ n$$

On a :

$$A_n^p = \frac{n!}{(n-p)!}.$$

(1) *$n!$ se lit « factorielle n ».*

◇ *Exemple 1.*

Soit l'ensemble E = { *a*; *b*; *c*; *d* }. Etudier les arrangements 2 à 2 des éléments de E.

Le nombre des arrangements est

$$A_4^2 = 4 \times 3 = 12.$$

On les obtient facilement :

(*a*; *b*)	(*b*; *a*)
(*a*; *c*)	(*c*; *a*)
(*a*; *d*)	(*d*; *a*)
(*b*; *c*)	(*c*; *b*)
(*b*; *d*)	(*d*; *b*)
(*c*; *d*)	(*d*; *c*).

◇ *Exemple 2.*

Soit l'ensemble E = { *a*; *b*; *c*; *d* }. Etudier les arrangements 3 à 3 des éléments de E.

Le nombre des arrangements est

$$A_4^3 = 4 \times 3 \times 2 = 24.$$

On les déduit des arrangements de l'exemple précédent en ajoutant à la fin des arrangements du tableau de l'exemple 1 un des deux éléments non utilisés.

(*a*; *b*; *c*)	(*a*; *b*; *d*)	(*b*; *a*; *c*)	(*b*; *a*; *d*)
(*a*; *c*; *b*)	(*a*; *c*; ;*d*)	(*c*; *a*; *b*)	(*c*; *a*; *d*)
(*a*; *d*; *b*)	(*a*; *d*; *c*)	(*d*; *a*; *b*)	(*d*; *a*; *c*)
(*b*; *c*; *a*)	(*b*; *c*; *d*)	(*c*; *b*; *a*)	(*c*; *b*; *d*)
(*b*; *d*; *a*)	(*b*; *d*; *c*)	(*d*; *b*; *a*)	(*d*; *b*; *c*)
(*c*; *d*; *a*)	(*c*; *d*; *b*)	(*d*; *c*; *a*)	(*d*; *c*; *b*).

130. Permutations.

On suppose maintenant que I = { 1; 2; ...; n }, c'est-à-dire p = n.

Les injections de I dans E sont maintenant des bijections de I sur E. L'image de I est une suite finie des n éléments de E.

Une telle suite est appelée une permutation des n éléments distincts de E.

On note P_n le nombre des permutations des *n* éléments de E. On a :

$$P_n = A_n^n$$

c'est-à-dire :

$$P_n = n(n-1) \times ... \times 2 \times 1$$

ou encore :

$$P_n = n!$$

◇ *Exemple 1.*

Soit l'ensemble $E = \{ a; b \}$. Etudier les permutations de E.

Le nombre des permutations est :

$$P_2 = 2! = 2$$

Ce sont :

$$(a; b) \qquad (b; a)$$

◇ *Exemple 2.*

Soit l'ensemble $E = \{ a; b; c \}$. Etudier les permutations de E.

Le nombre des permutations est :

$$P_3 = 3! = 3 \times 2 \times 1 = 6.$$

Ce sont :

$(a; b; c)$ $(b; a; c)$
$(a; c; b)$ $(c; a; b)$
$(b; c; a)$ $(c; b; a)$

131. Combinaisons.

Soit un ensemble E de n éléments distincts.

On appelle combinaison de ces n éléments p à p toute partie de l'ensemble E composée de p éléments distincts de E.

Une combinaison de p éléments fournit $p!$ arrangements de n éléments p à p, car dans une combinaison l'ordre des éléments n'intervient pas, mais il intervient dans les arrangements (qui sont des suites).

En désignant (1) par C_n^p le nombre des combinaisons de n éléments p à p, on a :

$$C_n^p = \frac{A_n^p}{p!}$$

c'est-à-dire :

$$C_n^p = \frac{n(n-1) \ ... \ (n-p+1)}{1 \times 2 \times \ ... \ \times p}.$$

On remarquera que le numérateur et le dénominateur ont le même nombre p de facteurs.

---

(1) Au lieu de C_n^p on note parfois $\binom{n}{p}$.

On a encore :

$$\mathbf{C_n^p = \frac{n!}{(n-p)!\,p!}}.$$

◇ *Exemple 1.*

Soit l'ensemble $E = \{a; b; c\}$. Etudier les combinaisons de deux éléments de E.

Le nombre des combinaisons est :

$$C_3^2 = \frac{3 \times 2}{1 \times 2} = 3.$$

Ce sont :

$$\{a; b\} \qquad \{a; c\} \qquad \{b; c\}$$

◇ *Exemple 2.*

Soit l'ensemble $E = \{a; b; c; d\}$. Etudier les combinaisons de deux éléments.

Le nombre des combinaisons est :

$$C_4^2 = \frac{4 \times 3}{1 \times 2} = 6.$$

Ce sont :

$$\{a; b\} \qquad \{a; c\} \qquad \{a; d\}$$
$$\{b; c\} \qquad \{b; d\}$$
$$\{c; d\}$$

132. Formules fondamentales.

1° On a :

$$C_n^p = \frac{n!}{(n-p)!\,p!}$$

et

$$C_n^{n-p} = \frac{n!}{p!\,(n-p)!}$$

D'où :

$$\mathbf{C_n^p = C_n^{n-p}}.$$

2° On a :

$$C_{n-1}^{p-1} + C_{n-1}^p = \frac{(n-1)!}{p!\,(n-p-1)!} + \frac{(n-1)!}{(p-1)!\,(n-p)!}$$
$$= \frac{(n-1)!}{p!\,(n-p)!} \cdot (n-p+p)$$
$$= \frac{n!}{p!\,(n-p)!}.$$

D'où la formule :

$$C_{n-1}^{p-1} + C_{n-1}^{p} = C_{n}^{p}.$$

3° On a :

$$C_n^n = \frac{n\,(n-1) \times \;\ldots\; 2 \times 1}{1 \times 2 \times \;\ldots\; (n-1)\,n} = 1$$

et d'autre part :

$$C_n^n = \frac{n!}{n!\,0!}.$$

D'où la convention :

$$0! = 1.$$

4° On a encore :

$$C_n^0 = \frac{n!}{n!\,0!}$$

D'où la convention :

$$C_n^0 = 1.$$

133. Le symbole Σ.

1° Soient les nombres :

$$a_1 \quad a_2 \ldots a_n$$

et leur somme :

$$S = a_1 + a_2 + \ldots + a_n$$

On note symboliquement :

$$S = \sum_{i=1}^{n} a_i$$

◇ *Exemple.*

Soit :

$$S = 1^2 + 2^2 + \ldots + n^2$$

On note :

$$S = \sum_{m=1}^{m=n} m^2$$

ou

$$S = \sum_{i=1}^{n} i^2.$$

2° Soient la suite finie à deux indices, dont les éléments sont disposés dans le tableau ci-contre.

Le tableau comprend n colonnes et p lignes.

a_{11}	a_{21}	a_{31}	----------	a_{n1}
a_{12}	a_{22}	a_{32}	----------	a_{n2}
a_{13}	a_{23}	a_{33}	----------	a_{n3}
-----	-----	-----	----------	-----
-----	-----	-----	----------	-----
a_{1p}	a_{2p}	a_{3p}	----------	a_{np}

La somme S des éléments du tableau est notée symboliquement.

$$\mathbf{S} = \sum_{\substack{i=1\\j=1}}^{\substack{j=p\\i=n}} \mathbf{a}_{ij}$$

On peut sommer les lignes; on a :

$$L_1 = a_{11} + a_{21} + \dots + a_{n1}$$

ou

$$L_1 = \sum_{i=1}^{i=n} a_{i1}.$$

De façon générale :

$$L_j = \sum_{=1}^{i=n} a_{ij}.$$

Et finalement $$\mathbf{S} = \sum_{j=1}^{j=p} \left[\sum_{i=1}^{i=n} \mathbf{a}_{ij} \right].$$

De même, en sommant par colonnes :

$$\mathbf{S} = \sum_{i=1}^{i=n} \left[\sum_{j=1}^{j=p} \mathbf{a}_{ij} \right].$$

On peut encore sommer les éléments des diagonales montantes :

$$D_2 = a_{11}$$
$$D_3 = a_{12} + a_{21}$$
$$D_4 = a_{13} + a_{22} + a_{31}$$
$$\dots\dots\dots\dots\dots\dots$$

D'où : $$\mathbf{D}_k = \sum_{i+j=k} \mathbf{a}_{ij}.$$

CHAPITRE XIV

NOMBRES NATURELS PREMIERS

134. Nombre premier.

1° ***Un nombre premier est un nombre n'admettant pas d'autre diviseur que lui-même et l'unité.***

◇ *Exemple.*

7 est premier, car 7 est divisible seulement par 1 et 7.

2° ***Un nombre qui n'est pas premier est dit nombre composé.***

◇ *Exemple.*

15 est un nombre composé, car $15 = 3 \times 5$ et 15 admet d'autres diviseurs que 1 et 15.

135. Plus petit diviseur d'un nombre.

Soit A un nombre composé; et soit d le plus petit de ses diviseurs ($d \neq 1$).

d est premier, sinon il serait composé et admettrait d_1, autre que 1 et d, qui serait inférieur à d; d_1 serait diviseur de A et d ne serait pas le plus petit diviseur de A; ce qui est contraire à l'hypothèse.

D'où :

Le plus petit diviseur, autre que 1, d'un nombre entier naturel composé est un nombre premier.

Par suite :

Tout nombre composé admet au moins un diviseur premier autre que l'unité et lui-même.

136. Décomposition multiplicative d'un nombre naturel composé.

Soient A un entier composé, et d son plus petit diviseur ($d \neq 1$).

On a :

$$A = d \cdot d_1$$

étant un nombre premier.
Si d_1 est premier, A est le produit de deux nombres premiers.
Si d_1 est composé, son plus petit diviseur d' est premier et $d = d' \cdot d_2$.

D'où :

$$A = d \cdot d' \cdot d_2.$$

Si d_2 est premier, A est le produit de trois nombres premiers.
Si d_2 est composé, on recommence le même raisonnement.
La suite $d, d_1, d_2 ...$, est une suite décroissante; le nombre de ses éléments est fini et le dernier des éléments est premier.

D'où :

Tout nombre composé est décomposable en un produit de nombres premiers.

Les facteurs premiers égaux peuvent se grouper en puissances, et le nombre A peut s'écrire :

$$A = a^{\alpha} \cdot b^{\beta} \ \ldots \ l^{\lambda}$$

a, b, ..., l *étant des nombres premiers et* $\alpha, \beta, \ldots \lambda$ *étant des entiers naturels.*

137. Unicité de la décomposition.

On envisage l'ensemble E des nombres naturels dont la décomposition n'est pas unique, et on se propose de montrer que cet ensemble est vide.

Soit A le plus petit nombre de l'ensemble E; il a au moins deux décompositions :

$$A = a^{\alpha} \cdot b^{\beta} \cdot l^{\lambda} = a'^{\alpha'} \cdots b'^{\beta'} \cdot l'^{\lambda'}.$$

1° *Les nombres premiers* a, b, ..., l, a', b' ... l' *sont différents.*

En effet si par exemple a et a' étaient égaux, le quotient A' de A par $a = a'$ posséderait deux décompositions.

$$A' = a^{\alpha-1} \cdot b^{\beta} \ldots l^{\lambda}$$
$$= a'^{\alpha'-1} \cdot b'^{\beta'} \ldots l'^{\lambda'}$$

et A ne serait pas le plus petit élément de E; ce qui est contraire à l'hypothèse.

En mettant a et a' en évidence le nombre A s'écrit alors :

$$A = a \cdot A_1 = a' \cdot A'_1$$

avec

$$A_1 = a^{\alpha-1} \cdot b^{\beta} \ldots l^{\lambda}$$

et

$$A'_1 = a'^{\alpha'-1} \cdot b'^{\beta'} \ldots l'^{\lambda'}.$$

2° *L'ensemble E est vide.*

a et a' étant différents, on peut supposer $a' > a$. La division euclidienne de a' par a donne

$$a' = aq + r$$

avec $r < a$, et $r \neq 0$ car a' est premier.

Donc :

$$A = a \cdot A_1 = (aq + r) \cdot A'_1.$$

On en déduit :

$$B = a\,(A_1 - q \cdot A'_1) = r \cdot A'_1.$$

Or a figure dans la première décomposition de B, mais ne figure pas dans la seconde ($a \neq r$) et a ne figure pas dans la décomposition de A'_1). Ainsi B aurait une double décomposition. B étant inférieur à A, ($B = A - aqA'_1$), A ne serait pas le plus petit élément de E; ce qui est contraire à l'hypothèse.

Donc :

Le résultat de la décomposition d'un nombre en un produit de facteurs premiers est unique.

138. Liste des nombres premiers inférieurs à 100.

Dans la suite des 100 premiers nombres entiers, on barre les multiples de 2 à partir de $2^2 = 4$; les multiples de 3 à partir de $3^2 = 9$; les multiples de 5 à partir de $5^2 = 25$; les multiples de 7 à partir de $7^2 = 49$. Les nombres non barrés sont des nombres premiers.

On obtient la liste suivante, dite Crible d'Erathostène :

1	**2**	**3**	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~	~~10~~
11	~~12~~	**13**	~~14~~	~~15~~	~~16~~	**17**	~~18~~	**19**	~~20~~
~~21~~	~~22~~	**23**	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	**29**	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	**37**	~~38~~	~~39~~	~~40~~
41	~~42~~	**43**	~~44~~	~~45~~	~~46~~	**47**	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	**53**	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	**59**	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	**67**	~~68~~	~~69~~	~~70~~
71	~~72~~	**73**	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	**79**	~~80~~
~~81~~	~~82~~	**83**	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	**89**	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	**97**	~~98~~	~~99~~	~~100~~

139. Reconnaître si un nombre est premier.

On cherche successivement si le nombre est divisible par les nombres premiers 2, 3, 5, 7... jusqu'à ce que l'on arrive, soit à une division exacte (alors le nombre est composé), soit à l'essai d'un nombre premier dont le carré est supérieur au nombre donné (alors le nombre est premier).

Pratiquement, on cesse les divisions lorsque le quotient devient inférieur au diviseur.

◇ *Exemple 1.*

Le nombre 113 est-il premier?

113 n'est pas divisible par 2; ni par 3; ni par 5; ni par 7; ni par 11. Comme $11^2 = 121$, on en déduit que 113 est un nombre premier.

◇ *Exemple 2.*

Le nombre 221 est-il premier?

221 n'est pas divisible par 2; ni par 3; ni par 5; ni par 7; ni par 11. Mais 221 est divisible par 13, et on a $221 = 13 \times 17$.

221 n'est donc pas un nombre premier.

140. Suite des nombres premiers.

On suppose que la suite des nombres premiers a été construite jusqu'au nombre premier p :

$$2; 3; 5; ...; p$$

Le nombre :

$$N = 2 \times 3 \times ... \times p + 1$$

n'est pas divisible par les nombres premiers de la suite construite, car le reste des divisions de N par les nombres de cette suite est 1.

Donc ou bien le nombre N est premier, ou bien son plus petit diviseur n'appartient pas à la suite construite. De toute façon, il existe un nombre premier supérieur à p.

Et :

La suite des nombres premiers n'est pas une suite finie.

141. Diviseurs primaires d'un nombre composé.

1° *Soit un nombre premier* a*; toute puissance* a^n *de* a *est appelé un nombre primaire.*

Ainsi :

$$2^3 \quad 5^2 \quad 7^4$$

sont des nombres primaires.

2° Si le nombre composé A s'écrit (de façon unique) sous la forme :

$$A = a^{\alpha} \cdot b^{\beta} \cdot c^{\gamma},$$

on dit que *A est décomposé en un produit de facteurs primaires.*

Ainsi :

$$\begin{aligned} A &= 360 \\ &= 2^3 \times 3^2 \times 5 \end{aligned}$$

est décomposé en un produit de facteurs primaires : 2^3; 3^2 et 5.

3° Soit le nombre :

$$A = a^{\alpha} \cdot b^{\beta} \cdot c^{\gamma}.$$

Le *tableau de ses diviseurs primaires* (c'est-à-dire de ses diviseurs qui sont des nombres primaires) est :

$$\left\{\begin{array}{llll} 1 & & & \\ a & a^2 & \dots & a^{\alpha} \\ b & b^2 & \dots & b^{\beta} \\ c & c^2 & \dots & c^{\gamma} \end{array}\right.$$

◇ *Exemple.*

On a : $360 = 2^3 \times 3^2 \times 5.$

Le tableau des diviseurs primaires de 360 est :

$$\left\{\begin{array}{lll} 1 & & \\ 2 & 2^2 & 2^3 \\ 3 & 3^2 & \\ 5 & & \end{array}\right.$$

4° *Un nombre est déterminé par un ensemble de facteurs primaires.*

Ainsi au tableau suivant de nombres primaires :

$$\left\{\begin{array}{lll} 1 & & \\ 2 & 2^2 & 2^3 \\ 3 & & \\ 5 & 5^2 & \end{array}\right.$$

est associé le nombre $A = 1 \times 2^3 \times 3 \times 5^2 = 600.$

5° *Bien entendu, dans un tableau de facteurs primaires aucune puissance intermédiaire ne doit manquer.*

Ainsi :

$$\left\{\begin{array}{ll} 1 & \\ 2 & 2^3 \\ 5 & \end{array}\right.$$

n'est pas un tableau de facteurs primaires, car la puissance 2^2 manque.

142. Diviseurs primaires d'un produit.

Soient les nombres

$$A = a^{\alpha} \cdot b^{\beta} \cdot c^{\gamma}$$

et

$$B = a^{\alpha'} \cdot b^{\beta'} \cdot c^{\gamma'}$$

Le produit M = AB est :

$$AB = a^{\alpha+\alpha'} \cdot b^{\beta+\beta'} \cdot c^{\gamma+\gamma'}$$

et l'ensemble des facteurs primaires de AB est :

$$\left\{\begin{array}{llll} 1 & & & \\ a & a^2 & \dots & a^{\alpha+\alpha'} \\ b & b^2 & \dots & b^{\beta+\beta'} \\ c & c^2 & \dots & c^{\gamma+\gamma'} \end{array}\right.$$

CHAPITRE XV

DIVISEURS D'UN NOMBRE

143. Définition.

***Si le nombre* a *divise exactement le nombre* b, *on dit que* a *est un diviseur de* b.**

On note :

$$a \mid b$$

et on lit « a *divise* b » *ou* « a *est diviseur de* b ».

Evidemment, on a l'implication :

$$(\mathbf{a} \mid \mathbf{b}) \Leftrightarrow [(\exists \mathbf{q}) : \mathbf{b} = \mathbf{aq}].$$

144. Relation d'ordre partiel.

La relation précédente notée* |, *introduit dans* N *une relation d'ordre partiel.

En effet, elle possède les propriétés suivantes :

Réflexivité.

Quel que soit a, a divise a.

R $\qquad (\forall a)\ a \mid a.$

Antisymétrie.

C'est-à-dire :

AS $\qquad (\forall a)\ (\forall b)\ (a \mid b \quad \text{et} \quad b \mid a) \Rightarrow a = b.$

En effet, de :

$$b = aq \quad \text{et} \quad a = bq'$$

on déduit :

$$ab = abqq'$$

d'où :

$$qq' = 1$$

et :

$$q = q' = 1.$$

Finalement, on a bien $a = b$.

Transivité.

C'est-à-dire :

T $(\forall a)\ (\forall b)\ (\forall c)\ (a \mid b \quad \text{et} \quad b \mid c) \Rightarrow a \mid c.$

En effet, de :

$$b = aq \quad \text{et} \quad c = bq'$$

on déduit, en remplaçant b dans la seconde égalité,

$$c = aqq';$$

ce qui signifie que a divise c.

L'ordre est partiel; si on considère, par exemple les nombres 3 et 7, 3 ne divise pas 7 et 7 ne divise pas 3; autrement dit, 3 et 7 ne sont pas comparables.

145. Ensemble des diviseurs d'un nombre.

1° *On désigne par Div A l'ensemble des diviseurs du nombre A.*

1 et A sont évidemment des diviseurs de A : ce sont les *diviseurs triviaux* de A.

2° Un diviseur de B est inférieur ou égal à B. Donc :

$$\boldsymbol{A \mid B \quad \Rightarrow \quad A \leqslant B.}$$

Il s'ensuit que le *nombre des diviseurs d'un nombre est fini.*

Des tables de diviseurs sont établies pour les nombres de 1 à 150; elles permettent d'abréger certains calculs.

3° Soit un nombre :

$$A = a^{\alpha} \cdot b^{\beta} \cdot c^{\gamma}$$

On considère le nombre $d = a^{\alpha'} \cdot b^{\beta'} \cdot c^{\gamma'}$ avec $\alpha' \leqslant \alpha$, $\beta' \leqslant \beta$; $\gamma' \leqslant \gamma$. Alors :

$$A = d \cdot A_1$$

avec $$A_1 = a^{\alpha-\alpha'} \times b^{\beta-\beta'} \times c^{\gamma-\gamma'}.$$

Donc d est un diviseur de A.

Réciproquement : *la décomposition en facteurs primaires de tout diviseur* d *de A est incluse dans celle de A.*

D'où :

> ***Une condition nécessaire et suffisante pour que* d *divise A est que la décomposition de* d *en facteurs primaires soit incluse dans celle de A.***

4° Ce résultat permet de trouver l'ensemble des diviseurs de A. Soit le tableau des diviseurs primaires de A :

$$\begin{cases} 1 \\ a & a^2 & \dots & a^\alpha \\ b & b^2 & \dots & b^\beta \\ c & c^2 & \dots & c^\gamma \end{cases}$$

On considère les ensembles :

$$L = \{ 1; a; a^2; \dots; a^\alpha \}$$
$$M = \{ 1; b; b^2; \dots; b^\beta \}$$
$$N = \{ 1; c; c^2; \dots; c^\gamma \}$$

> ***Les diviseurs de A sont les produits des éléments de chacun des éléments de l'ensemble L × M × N.***

◇ *Exemple.*

Soit $A = 180$
$= 2^2 \times 3^2 \times 5$

Le tableau des facteurs primaires est :

$$\begin{cases} 1 \\ 2 & 4 \\ 3 & 9 \\ 5 \end{cases}$$

D'où :

$$L = \{ 1; 2; 4 \}$$
$$M = \{ 1; 3; 9 \}$$
$$N = \{ 1; 5 \}$$

Les éléments de L × M × N fournissent les diviseurs de 180 :

$$L \times M \times N \begin{cases} \left.\begin{matrix} 1 & 2 & 4 \\ 3 & 6 & 12 \\ 9 & 18 & 36 \end{matrix}\right\} L \times M \\ \begin{matrix} 5 & 10 & 20 \\ 15 & 30 & 60 \\ 45 & 90 & 180 \end{matrix} \end{cases}$$

5° De plus, on a :

$$\text{Card}(L \times M \times N) = \text{Card}(L) \times \text{Card}(M) \times \text{Card}(N) = (1+\alpha)(1+\beta)(1+\gamma)$$

Le nombre des diviseurs de A $= a^{\alpha} b^{\beta} c^{\gamma}$ ***est donc*** $(1+\alpha)(1+\beta)(1+\gamma)$.

146. Propriétés principales des diviseurs.

1° On a l'implication :

$$(d \mid a \quad \text{et} \quad d \mid b) \Rightarrow d \mid a+b.$$

En effet de :

$$a = \alpha \cdot d \quad \text{et} \quad b = \beta d$$

on tire :

$$a + b = (\alpha + \beta) d$$

c'est-à-dire :

$$d \mid a + b.$$

2° On a, de même, si $a \geqslant b$:

$$(d \mid a \quad \text{et} \quad d \mid b) \Rightarrow d \mid a-b.$$

3° Et aussi, si $n \in N$:

$$d \mid a \Rightarrow d \mid na$$

et

$$d \mid a \Rightarrow d \mid a^n.$$

CHAPITRE XVI

PLUS GRAND COMMUN DIVISEUR

147. Diviseurs communs de deux nombres.

Etant donnés deux nombres A et B, un nombre d est diviseur commun de ces deux nombres s'il les divise tous les deux.

◇ *Exemple 1.*

Soient les nombres $A = 120$ et $B = 56$. Les nombres 2, 4, 8 sont des diviseurs communs de 120 et 56.

◇ *Exemple 2.*

Soient les nombres $A = 12$ et $B = 48$. Le nombre 12 est un diviseur commun de 12 et 48.

148. Plus grand commun diviseur de deux nombres.

Les diviseurs communs de deux nombres ne peuvent être supérieurs au plus petit de ces deux nombres.

Il existe donc un diviseur commun qui est supérieur à tous les autres diviseurs. C'est le *plus grand commun diviseur;* on le désigne par le sigle P.G.C.D.

149. Opération P.G.C.D.

A deux nombres entiers naturels A et B on fait correspondre le P.G.C.D. Δ de ces deux nombres. On définit ainsi une loi de composition interne dans N.

f : $(A;B) \in N^2 \longrightarrow f(A;B) = \Delta \in N.$

On note :

$$A \wedge B = \Delta$$

et on lit « *A* pgcd *B* ».

◇ *Exemple 1.*

Soient les nombres A = 18 et B = 27. Leur P.G.C.D. est $\Delta = 9$. On a donc :

$$18 \wedge 27 = 9.$$

◇ *Exemple 2.*

Soient les nombres A = 84 et B = 120. On a :

$$84 \wedge 120 = 12.$$

150. Recherche du P.G.C.D. de deux nombres.

1° Soient les deux nombres A = 84 et B = 120.

L'ensemble A′ des diviseurs primaires de 84 est :

$$A' : \begin{cases} 1 \\ 2 \quad 2^2 \\ 3 \\ 7 \end{cases}$$

L'ensemble B′ des diviseurs primaires de 120 est :

$$B' : \begin{cases} 1 \\ 2 \quad 2^2 \quad 2^3 \\ 3 \\ 5 \end{cases}$$

L'intersection $A' \cap B'$ de ces deux ensembles est :

$$\Delta' = A' \cap B' \begin{cases} 1 \\ 2 \quad 2^2 \\ 3 \end{cases}$$

Ce tableau Δ' est le tableau des diviseurs primaires du nombre

$$\Delta = 1 \times 2^2 \times 3$$
$$= 12.$$

Ce nombre Δ est diviseur commun à A et B, et c'est le plus grand des diviseurs d'après sa formation à l'aide d'une intersection.

2° Plus généralement soient les deux nombres :

$$A = a^{\alpha} b^{\beta} c^{\gamma}$$

et

$$B = a^{\alpha'} b^{\beta'} c^{\gamma'}.$$

L'ensemble A' des diviseurs primaires de A est :

$$A' \begin{cases} 1 \\ a \quad a^2 \quad \dots \quad a^\alpha \\ b \quad b^2 \quad \dots \quad b^\beta \\ c \quad c^2 \quad \dots \quad c^\gamma \end{cases}$$

L'ensemble B' des diviseurs primaires de B est :

$$B' \begin{cases} 1 \\ a \quad a^2 \quad \dots \quad a^{\alpha'} \\ b \quad b^2 \quad \dots \quad b^{\beta'} \\ c \quad c^2 \quad \dots \quad c^{\gamma'} \end{cases}$$

L'intersection $\Delta' = A' \cap B'$ de ces deux ensembles est :

$$\Delta' = A' \cap B' : \begin{cases} 1 \\ a \quad a^2 \quad \dots \quad a^r \\ b \quad b^2 \quad \dots \quad b^s \\ c \quad c^2 \quad \dots \quad c^t \end{cases}$$

avec

$$r = \operatorname{Inf}(\alpha ; \alpha')$$
$$s = \operatorname{Inf}(\beta ; \beta')$$
$$t = \operatorname{Inf}(\gamma ; \gamma')$$

Ce tableau Δ' est le tableau des diviseurs primaires du nombre

$$\Delta = a^r \cdot b^s \cdot c^t.$$

L'intersection Δ' étant la plus grande partie contenue dans A et B, il s'ensuit que Δ est le P.G.C.D. de A et B.

151. Remarque.

Le signe $\wedge$ de l'opération P.G.C.D. a été choisi pour rappeler l'intersection $A' \cap B'$ utilisée pour trouver $\Delta = A \wedge B$.

152. Commutativité.

De l'égalité :

$$A' \cap B' = B' \cap A'$$

on déduit :

$$A \wedge B = B \wedge A.$$

Et :

L'opération P.G.C.D. est commutative.

153. Idempotence.

1° De l'égalité :

$$A' \cap A' = A'$$

on déduit :

$$\boldsymbol{A \wedge A = A.}$$

Et :

L'opération P.G.C.D. est idempotente.

2° Soient les nombres A et B = $k \cdot A$ ($k \in N$). Comme A est diviseur de B = kA, A est le P.G.C.D. de A et B.

Et :

$$\boldsymbol{A \wedge kA = A.} \qquad (153\,;\,1)$$

154. P.G.C.D. et divisibilité.

Si A divise B, on a B = $k \cdot A$, et ainsi $A \wedge B = A$.
Réciproquement si A est le P.G.C.D. de A et B, A divise évidemment B.

Finalement, on a donc l'équivalence

$$\boldsymbol{A | B \iff A \wedge B = A.}$$

155. Associativité.

1° Soient trois nombres A, B, C; et A′, B′, C′ leurs ensembles de diviseurs primaires.

De l'égalité :

$$(A' \cap B') \cap C' = A' \cap (B' \cap C')$$

on déduit :

$$\boldsymbol{(A \wedge B) \wedge C = A \wedge (B \wedge C).}$$

Et :

L'opération P.G.C.D. est associative.

On peut écrire :

$$\Delta = (A \wedge B) \wedge C = A \wedge (B \wedge C) = A \wedge B \wedge C.$$

2° On peut évidemment généraliser à plus de trois nombres, et *le P.G.C.D. est une opération commutative et associative.*

3° ***Soient les nombres***

$$\mathbf{A = a^{\alpha} \cdot b^{\beta} c^{\gamma}}$$
$$\mathbf{B = a^{\alpha'} b^{\beta'} c^{\gamma'}}$$
$$\mathbf{C = a^{\alpha''} b^{\beta''} c^{\gamma''}}$$

Leur P.G.C.D. est :

$$\mathbf{\Delta = a^r b^s c^t}$$

avec :

$$\mathbf{r = Inf\,(\alpha;\ \alpha';\ \alpha'')}$$
$$\mathbf{s = Inf\,(\beta;\ \beta';\ \beta'')}$$
$$\mathbf{t = Inf\,(\gamma;\ \gamma';\ \gamma'')}$$

◇ *Exemple.*

Soient les nombres :

$$A = 240 = 2^4 \times 3 \times 5$$
$$B = 28 = 2^2 \times 7$$
$$C = 440 = 2^3 \times 5 \times 11$$

D'où, d'après la règle précédente :

$$\Delta = A \wedge B \wedge C = 2^2 = 4.$$

156. Distributivité de la multiplication pour le P.G.C.D.

Soient les trois nombres A, B, C. On se propose de démontrer la formule :

$$\boldsymbol{C \cdot (A \wedge B) = CA \wedge CB.}$$

Si on a :

$$A = a^{\alpha} b^{\beta} c^{\gamma}$$
$$B = a^{\alpha'} b^{\beta'} c^{\gamma'}$$
$$C = a^{\alpha''} b^{\beta''} c^{\gamma''}$$

on en déduit :

$$A \wedge B = a^r\, b^s\, c^t$$

avec :

$$r = \text{Inf}\,(\alpha;\ \alpha'), \quad s = \text{Inf}\,(\beta;\ \beta'), \quad t = \text{Inf}\,(\gamma;\ \gamma').$$

D'où :

$$C \cdot (A \wedge B) = a^{r+\alpha''} \cdot b^{s+\beta''} \cdot c^{t+\gamma''}$$

D'autre part :

$$CA = a^{\alpha+\alpha''} \cdot b^{\beta+\beta''} \cdot c^{\gamma+\gamma''}$$

et

$$CB = a^{\alpha'+\alpha''} \cdot b^{\beta'+\beta''} \cdot c^{\gamma'+\gamma''}.$$

D'où :

$$CA \wedge CB = a^{r'} \cdot b^{s'} \cdot c^{t'}$$

avec :

$$r' = \text{Inf}(\alpha + \alpha''; \alpha' + \alpha''), \qquad s' = \text{Inf}(\beta + \beta''; \beta' + \beta''),$$
$$t' = \text{Inf}(\gamma + \gamma''; \gamma' + \gamma'')$$

Or : $r + \alpha'' = r', \quad s + \beta'' = s', \quad t + \gamma'' = t'$ puisque :

$$\alpha'' + \text{Inf}(\alpha; \alpha') = \text{Inf}(\alpha + \alpha''; \alpha' + \alpha'')$$
$$\beta'' + \text{Inf}(\beta; \beta') = \text{Inf}(\beta + \beta''; \beta' + \beta'')$$
$$\gamma'' + \text{Inf}(\gamma; \gamma') = \text{Inf}(\gamma + \gamma''; \gamma' + \gamma'')$$

Donc :

$$C \cdot (A \wedge B) = CA \wedge CB.$$

Et :

La multiplication est distributive pour le P.G.C.D.

ou encore :

Si les nombres A et B ont pour P.G.C.D. Δ, alors les nombres CA et CB ont pour P.G.C.D. $C\Delta$.

157. P.G.C.D. de A et BC.

En désignant par $\dfrac{A}{A \wedge B}$ le quotient de A par le P.G.C.D. de A et B, on a :

$$\left(\frac{A}{A \wedge B} \wedge C\right) \cdot (A \wedge B) = A \wedge [C \cdot (A \wedge B)] \quad \text{(Distributivité)}$$
$$= A \wedge (CA \wedge CB) \quad \text{(Distributivité)}$$
$$= (A \wedge CA) \wedge CB \quad \text{(Associativité)}$$
$$= A \wedge BC \quad \text{(Formule 153; 1)}$$

D'où la formule fondamentale.

$$A \wedge BC = \left(\frac{A}{A \wedge B} \wedge C\right) \cdot (A \wedge B). \qquad (157;\ 1)$$

On a aussi :

$$A \wedge BC = \left(\frac{A}{A \wedge C} \wedge B\right) \cdot (A \wedge C). \qquad (157;\ 2)$$

158. Relation entre l'addition et le P.G.C.D.

Soient les deux nombres :

$$M = A \wedge B$$

et

$$N = A \wedge (B + nA) \qquad (n \in N)$$

On désigne par μ l'ensemble des diviseurs de $M = A \wedge B$ et par ν l'ensemble des diviseurs de $N = A \wedge (B + nA)$.

Tout diviseur de M est diviseur de A et B, donc diviseur de $B + nA$; c'est donc un diviseur commun de A et $B + nA$, c'est-à-dire un diviseur de N. Par suite :

$$\mu \subset \nu$$

Tout diviseur de N est diviseur de A et $B + nA$, donc diviseur de A et B; c'est un diviseur de M. Donc :

$$\nu \subset \mu$$

On en déduit :

$$\mu = \nu$$

c'est-à-dire : $M = N$.

D'où la formule :

$$\boldsymbol{A \wedge (B + nA) = A \wedge B.}$$

159. Algorithme d'Euclide.

Soient deux nombres A et B, avec $A > B$.

On appelle algorithme d'Euclide, la suite de divisions :

$$\begin{array}{ll}
A = BQ + R_1 & R_1 < B \\
B = R_1Q_1 + R_2 & R_2 < R_1 \\
R_1 = R_2Q_2 + R_3 & R_3 < R_2 \\
R_2 = R_3Q_3 + R_4 & R_4 < R_3 \\
\dots\dots\dots\dots & \\
R_{n-2} = R_{n-1}\,Q_{n-1} + R_n & R_n < R_{n-1} \\
R_{n-1} = R_nQ_n. &
\end{array}$$

La suite B, R_1, R_2, ..., R_n est strictement décroissante et finie; on aboutit donc bien à la division exacte $R_{n-1} = R_n Q_n$.

D'après le théorème précédent :

$$A \wedge B = B \wedge R_1 = R_1 \wedge R_2 = \ \dots \ = R_{n-1} \wedge R_n = R_n.$$

D'où :

Le P.G.C.D. de deux nombres est le dernier reste non nul de l'algorithme d'Euclide.

◇ *Exemple.*

Soient les nombres $A = 120$ et $B = 84$. Calculer leur P.G.C.D. par l'algorithme d'Euclide.

On a :

$$120 = 84 \times 1 + 36$$
$$84 = 36 \times 2 + 12$$
$$36 = 12 \times 3.$$

Donc

$$\Delta = 120 \wedge 84 = 12.$$

CHAPITRE XVII

NOMBRES PREMIERS ENTRE EUX

160. Nombres premiers entre eux.

1° ***Deux nombres sont premiers entre eux si leur P.G.C.D. est l'unité.***

Par exemple, 15 et 154 sont des nombres premiers entre eux, car $15 \wedge 154 = 1$.

2° ***Plusieurs nombres sont premiers entre eux dans leur ensemble si leur P.G.C.D. est l'unité.***

Par exemple, 15, 25 et 9 sont des nombres premiers entre eux dans leur ensemble, car $15 \wedge 25 \wedge 9 = 1$.

3° ***Plusieurs nombres sont premiers entre eux, deux à deux, si deux quelconques d'entre eux sont premiers entre eux.***

Par exemple, 8, 9 et 35 sont des nombres premiers entre eux deux à deux, car $8 \wedge 9 = 1$, $8 \wedge 35 = 1$ et $9 \wedge 35 = 1$.

161. Propriétés des nombres premiers entre eux.

1° ***Si deux nombres A et B sont premiers entre eux, tout diviseur C de l'un A est premier avec l'autre B.***

On a :

$$A \wedge B = 1$$

et

$$C | A \Rightarrow C \wedge A = C$$

D'où :

$$\begin{aligned} C \wedge B &= (C \wedge A) \wedge B \\ &= C \wedge (A \wedge B) \\ &= C \wedge 1 \\ &= 1. \end{aligned}$$

Autrement dit, B et C sont premiers entre eux.

On a donc démontré l'implication :

$$\begin{pmatrix} & A \wedge B = 1 \\ \text{et} & \\ & C \mid A \end{pmatrix} \Rightarrow (C \wedge B = 1).$$

2° ***On ne change pas le P.G.C.D. de deux nombres A et B si l'on multiplie l'un d'eux A par un nombre C premier avec l'autre B.***

On a :

$$C \wedge B = 1.$$

D'où :

$$\text{P.G.C.D. } (B\,; AC) = B \wedge AC = \left(\frac{B}{B \wedge C} \wedge A\right)(C \wedge B)$$

(cf. formule 157 ; 1)

$$= (B \wedge A) \cdot 1$$
$$= B \wedge A$$
$$= \text{P.G.C.D. } (A\,; B).$$

On a donc démontré l'implication :

$$(C \wedge B = 1) \quad \Rightarrow \quad (A \wedge B = CA \wedge B.)$$

3° ***Si le nombre C divise un produit AB de deux facteurs A et B premiers entre eux, et si ce nombre C est premier avec l'un d'eux A, alors il divise l'autre B.***

C étant premier avec A, on a :

$$C \wedge A = 1$$

$$C \wedge AB = \left(\frac{C}{C \wedge A} \wedge B\right) \cdot (C \wedge A)$$

ou

$$C \wedge AB = C \wedge B.$$

Or, d'autre part, C divisant AB le P.G.C.D. de C et AB est C :

$$C \wedge AB = C.$$

En comparant les deux résultats obtenus, on a :

$$C \wedge B = C$$

c'est-à-dire C divise B.

On a donc démontré l'implication :

$$(C \mid AB \quad \text{et} \quad C \wedge A = 1) \Rightarrow (C \mid B).$$

4° ***Si un nombre C est premier avec deux nombres A et B, alors C est premier avec le produit AB des deux nombres.***

On a par hypothèse :

$$C \wedge A = 1 \quad \text{et} \quad C \wedge B = 1.$$

D'autre part :

$$\begin{aligned} C \wedge AB &= \left(\frac{C}{C \wedge A} \wedge B\right) \cdot (C \wedge A) \\ &= C \wedge B \\ &= 1. \end{aligned}$$

Autrement dit, C est premier avec AB.

On a donc démontré l'implication :

$$(C \wedge A = 1 \quad \text{et} \quad C \wedge B = 1) \Rightarrow (C \wedge AB = 1).$$

5° ***Si un nombre C est premier avec le produit AB, alors C est premier avec A et avec B.***

On a :

$$C \wedge AB = 1.$$

Or :

$$C \wedge AB = \left(\frac{C}{C \wedge A} \wedge B\right) \cdot (C \wedge A)$$

et donc :

$$\left(\frac{C}{C \wedge A} \wedge B\right) \cdot (C \wedge A) = 1.$$

Par suite de la décomposition de 1 en facteurs unités, on a :

$$C \wedge A = 1.$$

On montre de même que :

$$C \wedge B = 1.$$

Autrement dit, C est premier avec A et avec B.

On a donc démontré l'implication.

$$(C \wedge AB = 1) \Rightarrow (C \wedge A = 1 \quad \text{et} \quad C \wedge B = 1).$$

6° ***Si A et B sont premiers entre eux, alors A est premier avec B^n.***

Autrement dit :

$$(A \wedge B = 1) \quad \Rightarrow \quad (A \wedge B^n = 1).$$

Ce résultat se démontre par une récurrence portant sur n.
D'après la seconde propriété :

$$A \wedge B = 1 \Rightarrow A \wedge B^2 = 1.$$

Autrement dit P(2) est vraie.

D'autre part, encore d'après la seconde propriété :

$$A \wedge B^n = 1 \Rightarrow A \wedge B^{n+1} = 1.$$

Ainsi :

$$P(n) \text{ vraie} \Rightarrow P(n+1) \text{ vraie}.$$

Donc par récurrence :

$$A \wedge B = 1 \Rightarrow A \wedge B^n = 1.$$

7° ***Si A et B sont premiers entre eux, alors A^p et B^n sont premiers entre eux.***

En effet, d'après la propriété précédente :

$$(A \wedge B = 1) \quad \Rightarrow \quad (A \wedge B^n = 1)$$

et

$$(A \wedge B^n = 1) \quad \Rightarrow \quad (A^p \wedge B^n = 1)$$

Autrement dit :

$$A \wedge B = 1 \Rightarrow A^p \wedge B^n = 1.$$

8° ***Si les nombres B et C sont premiers entre eux, alors le produit du P.G.C.D. de A et B et du P.G.C.D. de A et C est égal au P.G.C.D. de A et BC.***

En effet, on a :

$$\begin{aligned} (A \wedge B)\,(A \wedge C) &= [(A \wedge B) \cdot A] \wedge [(A \wedge B) \cdot C] && \text{(Distributivité)} \\ &= [(A \wedge B) \cdot A] \wedge [AC \wedge BC] && \text{(Distributivité)} \\ &= \{\, [(A \wedge B) \cdot A] \wedge AC \,\} \wedge BC && \text{(Associativité)} \\ &= A\,[(A \wedge B) \wedge C] \wedge BC && \text{(Distributivité)} \\ &= A\,[A \wedge (B \wedge C)] \wedge BC && \text{(Associativité)} \\ &= A\,[A \wedge 1] \wedge BC \\ &= (A \cdot 1) \wedge BC \\ &= A \wedge BC. \end{aligned}$$

On a donc démontré l'implication :

$$B \wedge C = 1 \Rightarrow (A \wedge B)\,(A \wedge C) = A \wedge BC.$$

9° ***Si M est divisible par A et par B, et si A et B sont premiers entre eux, alors M est divisible par AB.***

D'après la propriété précédente :

$$\begin{aligned} M \wedge AB &= (M \wedge A)\,(M \wedge B) \\ &= A \cdot B. \end{aligned}$$

car $M \wedge A = A$ puisque M est divisible par A, et $M \wedge B = B$ puisque M est divisible par B.

Enfin, l'égalité $M \wedge AB = AB$ montre que M est divisible par AB.

On a donc démontré l'implication :

$$(A|M \quad \text{et} \quad B|M \quad \text{et} \quad A \wedge B = 1) \Rightarrow (AB|M).$$

10° ***On généralise le théorème précédent :***

$$\begin{pmatrix} A|M, B|M, C|M \\ \text{et} \quad A \wedge B = 1, \\ A \wedge C = 1, \\ B \wedge C = 1 \end{pmatrix} \Rightarrow ABC|M.$$

11° ***Si le nombre X est premier séparément avec les nombres A et B, alors il est premier avec le produit AB.***

On a :

$$X \wedge A = 1 \qquad X \wedge B = 1.$$

D'où :

$$\begin{aligned} X \wedge AB &= \left(\frac{X}{X \wedge A} \wedge B\right)(X \wedge A) \\ &= (X \wedge A) \times 1 \\ &= 1. \end{aligned}$$

Donc X est premier avec AB.

On a donc démontré l'implication :

$$(X \wedge A = 1 \quad \text{et} \quad X \wedge B = 1) \Rightarrow X \wedge AB = 1.$$

On peut généraliser à plus de deux nombres :

$$(X \wedge A = 1; X \wedge B = 1; X \wedge C = 1) \Rightarrow X \wedge ABC = 1$$

et énoncer :

Si un nombre est premier avec chaque facteur d'un produit, alors il est premier avec ce produit.

CHAPITRE XVIII

PLUS PETIT COMMUN MULTIPLE

162. Multiples communs de deux nombres.

Etant donnés deux nombres A et B, un nombre M est multiple commun de ces nombres s'il est multiple de chacun d'eux.

◇ *Exemple.*

700 est multiple commun de $A = 4$ et $B = 14$.
L'ensemble des multiples communs de A et B n'est pas vide car il contient AB.

163. Plus petit commun multiple de deux nombres.

Les multiples communs des nombres A et B ne peuvent être inférieurs au plus grand de ces deux nombres. Il existe donc un multiple commun qui est inférieur à tous les autres. C'est le *plus petit commun multiple;* on le désigne par le sigle P.P.C.M.

164. Opération P.P.C.M.

A deux nombres entiers naturels A et B on fait correspondre le P.P.C.M. μ de ces deux nombres. On définit ainsi une loi de composition interne dans N :

f : $$(A\,;B) \in N^2 \longrightarrow f(A\,;B) = \mu \in N.$$

On note :

$$A \vee B = \mu$$

et on lit « *A* ppcm *B* ».

◇ *Exemple.*

Soient les nombres $A = 18$ et $B = 27$. Leur P.P.C.M. est $\mu = 54$. On a donc :

$$18 \vee 27 = 54.$$

165. Recherche du P.P.C.M. de deux nombres.

1° Soient les deux nombres A = 30 et B = 20.

L'ensemble A' des diviseurs primaires de A = 30 est :

$$A' : \begin{cases} 1 \\ 2 \\ 3 \\ 5 \end{cases}$$

L'ensemble B' des diviseurs primaires de B = 20 est :

$$B' : \begin{cases} 1 \\ 2 \quad 2^2 \\ 5 \end{cases}$$

La réunion $\mu' = A' \cup B'$ de ces deux ensembles est :

$$\mu' = A' \cup B' : \begin{cases} 1 \\ 2 \quad 2^2 \\ 3 \\ 5 \end{cases}$$

Ce tableau μ' est le tableau des diviseurs primaires du nombre

$$\mu = 1 \times 2^2 \times 3 \times 5$$
$$= 60.$$

Ce nombre μ est multiple commun à A et B, et c'est le plus petit des multiples communs d'après sa formation à l'aide d'une réunion.

2° Plus généralement, soient les deux nombres :

$$A = a^{\alpha} b^{\beta} c^{\gamma}$$

et

$$B = a^{\alpha'} b^{\beta'} c^{\gamma'}.$$

L'ensemble A' des diviseurs primaires de A est :

$$A' : \begin{cases} 1 \\ a \quad a^2 \quad \ldots \quad a^{\alpha} \\ b \quad b^2 \quad \ldots \quad b^{\beta} \\ c \quad c^2 \quad \ldots \quad c^{\gamma} \end{cases}$$

L'ensemble B' des diviseurs primaires de A est :

$$B' : \begin{cases} 1 \\ a \quad a^2 \quad \ldots \quad a^{\alpha'} \\ b \quad b^2 \quad \ldots \quad b^{\beta'} \\ c \quad c^2 \quad \ldots \quad c^{\gamma'} \end{cases}$$

La réunion $\mu' = A' \cup B'$ de ces deux ensembles est :

$$\mu' = A' \cup B' : \begin{cases} 1 \\ a \quad a^2 \quad \dots \quad a^r \\ b \quad b^2 \quad \dots \quad b^s \\ c \quad c^2 \quad \dots \quad c^t \end{cases}$$

avec :

$$r = \text{Sup}(\alpha ; \alpha')$$
$$s = \text{Sup}(\beta ; \beta')$$
$$t = \text{Sup}(\gamma ; \gamma')$$

Ce tableau μ' est le tableau des diviseurs primaires du nombre :

$$\mu = a^r b^s c^t.$$

La réunion μ' étant le plus petit ensemble contenant A et B, il s'ensuit que μ est le P.P.C.M. de A et B.

166. Remarque.

Le signe $\vee$ de l'opération P.P.C.M. a été choisi pour rappeler la réunion $A' \cup B'$ utilisée pour trouver $\mu = A \vee B$.

167. Commutativité.

De l'égalité :

$$A' \cup B' = B' \cup A'$$

on déduit :

$$A \vee B = B \vee A.$$

Et :

L'opération P.P.C.M. est commutative.

168. Idempotence.

1° De l'égalité :

$$A' \cup A' = A'$$

on déduit :

$$A \vee A = A$$

Et :

L'opération P.P.C.M. est idempotente.

2° Soient les nombres A et $B = kA$. ($k \in N$). Comme B est multiple de A, B est le P.P.C.M. de A et B.

Et :

$$\boldsymbol{A \vee kA = kA.} \qquad (168\,;\,1)$$

169. P.P.C.M. et divisibilité.

Si A divise B, on a $B = kA$, et ainsi $A \vee B = B$.
Réciproquement, si B est le P.P.C.M. de A et B, A divise évidemment B.

Finalement, on a l'équivalence :

$$A | B \iff A \vee B = B.$$

170. Associativité.

1° Soient trois nombres A, B, C; et A′, B′, C′ leurs ensembles de diviseurs primaires.

De l'égalité :

$$(A' \cup B') \cup C' = A' \cup (B' \cup C')$$

on déduit :

$$(A \vee B) \vee C = A \vee (B \vee C)$$

Et :

L'opération P.P.C.M. est associative.

On peut écrire :

$$\mu = (A \vee B) \vee C = A \vee (B \vee C) = A \vee B \vee C.$$

2° On peut évidemment généraliser à plus de trois nombres, et *le P.P.C.M. est une opération commutative et associative.*

3° *Soient les nombres :*

$$A = a^{\alpha} b^{\beta} c^{\gamma}$$
$$B = a^{\alpha'} b^{\beta'} c^{\gamma'}$$
$$C = a^{\alpha''} b^{\beta''} c^{\gamma''}.$$

Leur P.P.C.M. est :

$$\mu = a^r b^s c^t$$

avec :

$$r = \mathrm{Sup}(\alpha ; \alpha' ; \alpha'')$$
$$s = \mathrm{Sup}(\beta ; \beta' ; \beta'')$$
$$t = \mathrm{Sup}(\gamma ; \gamma' ; \gamma'')$$

◇ *Exemple.*

Soient les nombres :

$$A = 4 = 2^2$$
$$B = 14 = 2 \times 7$$
$$C = 10 = 2 \times 5.$$

D'où, d'après la règle précédente :

$$\mu = 2^2 \times 5 \times 7 = 140.$$

171. Distributivité de la multiplication pour le P.P.C.M.

Soient les trois nombres A, B, C. On se propose de démontrer la formule :

$$C \cdot (A \vee B) = CA \vee CB$$

Si on a :

$$A = a^{\alpha} b^{\beta} c^{\gamma}$$
$$B = a^{\alpha'} b^{\beta'} c^{\gamma'}$$
$$C = a^{\alpha''} b^{\beta''} c^{\gamma''}$$

on en déduit :

$$A \vee B = a^{r} b^{s} c^{t}$$

avec :

$$r = \text{Sup}(\alpha; \alpha'), \quad s = \text{Sup}(\beta; \beta'), \quad t = \text{Sup}(\gamma; \gamma').$$

D'où :

$$C\ (A \vee B) = a^{r+\alpha''} \cdot b^{s+\beta''} \cdot c^{t+\gamma''}$$

D'autre part :

$$CA = a^{\alpha+\alpha''} \cdot b^{\beta+\beta''} \cdot c^{\gamma+\gamma''}$$

et

$$CB = a^{\alpha'+\alpha''} \cdot b^{\beta'+\beta''} \cdot c^{\gamma'+\gamma''}$$

D'où :

$$CA \vee CB = a^{r'} \cdot b^{s'} \cdot c^{t'}$$

avec :

$$r' = \text{Sup}\ (\alpha + \alpha''; \alpha' + \alpha''), \quad s' = \text{Sup}\ (\beta + \beta''; \beta' + \beta'');$$
$$t' = \text{Sup}\ (\gamma + \gamma''; \gamma' + \gamma'')$$

Or :

$$r + \alpha'' = r', \quad s + \beta'' = s', \quad t + \gamma'' = t'$$

puisque

$$\alpha'' + \text{Sup}(\alpha; \alpha') = \text{Sup}(\alpha + \alpha''; \alpha' + \alpha'')$$
$$\beta'' + \text{Sup}(\beta; \beta') = \text{Sup}(\beta + \beta''; \beta' + \beta'')$$
$$\gamma'' + \text{Sup}(\gamma; \gamma') = \text{Sup}(\gamma + \gamma''; \gamma' + \gamma'').$$

Donc :

$$C \cdot (A \vee B) = CA \vee CB.$$

Et :

La multiplication est distributive pour le P.P.C.M.

ou encore :

Si les nombres A et B ont pour P.P.C.M. μ, alors les nombres CA et CB ont pour P.P.C.M. Cμ.

CHAPITRE XIX

RELATIONS ENTRE P.G.C.D ET P.P.C.M.

172. Relation entre le P.G.C.D. et le P.P.C.M. de deux nombres.

Soient les deux nombres

$$A = a^{\alpha} b^{\beta} c^{\gamma}$$
$$B = a^{\alpha'} b^{\beta'} c^{\gamma'}$$

Leur produit est :

$$AB = a^{\alpha+\alpha'} \cdot b^{\beta+\beta'} \cdot c^{\gamma+\gamma'}.$$

Leur P.G.C.D. est

$$\Delta = a^r b^s c^t$$

avec :

$$r = \text{Inf}(\alpha;\ \alpha'); \quad s = \text{Inf}(\beta;\ \beta'); \quad t = \text{Inf}(\gamma;\ \gamma').$$

Leur P.P.C.M. est

$$\mu = a^{r'} b^{s'} c^{t'}$$

avec :

$$r' = \text{Sup}(\alpha;\ \alpha'); \quad s' = \text{Sup}(\beta;\ \beta'); \quad t' = \text{Sup}(\gamma;\ \gamma').$$

Par suite le produit du P.P.C.M. et du P.G.C.D. est

$$\Delta \cdot \mu = a^{r+r'} \cdot b^{s+s'} \cdot c^{t+t'}.$$

Or :

$$\alpha + \alpha' = \text{Inf}(\alpha;\alpha') + \text{Sup}(\alpha;\alpha') = r + r'$$
$$\beta + \beta' = \text{Inf}(\beta;\beta') + \text{Sup}(\beta;\beta') = s + s'$$
$$\gamma + \gamma' = \text{Inf}(\gamma;\gamma') + \text{Sup}(\gamma;\gamma') = t + t'$$

c'est-à-dire que :

$$AB = \Delta \cdot \mu$$

Et :

Le produit de deux nombres est égal au produit de leur P.G.C.D. et de leur P.P.C.M.

On peut encore écrire :

$$A \cdot B = (A \wedge B) \cdot (A \vee B)$$

173. P.P.C.M. de deux nombres premiers entre eux.

Si les nombres A et B sont premiers entre eux, on a $\Delta = 1$ et par suite $AB = \mu$. Et :

Le P.P.C.M. de deux nombres premiers entre eux est égal à leur produit.

174. Quotients de deux nombres par leur P.G.C.D.

Soient les deux nombres A et B, et leur P.G.C.D. $\Delta = A \wedge B$.

On a :

$$A = \Delta \cdot A_1 \quad \text{et} \quad B = \Delta \cdot B_1$$

A_1 et B_1 sont les quotients de A et B par Δ.

D'où :

$$A \wedge B = \Delta A_1 \wedge \Delta B_1$$

ou

$$\Delta = \Delta\ (A_1 \wedge B_1)$$

et finalement :

$$1 = A_1 \wedge B_1$$

Et :

Les quotients de deux nombres par leur P.G.C.D. sont premiers entre eux.

175. Quotients du P.P.C.M. de deux nombres par ces nombres.

Soient les deux nombres A et B, et leur P.P.C.M. $\mu = A \vee B$.

On a :

$$\mu = A \cdot A_2 \quad \text{et} \quad \mu = B \cdot B_2$$

A_2 et B_2 sont les quotients de μ par A et par B.

D'où :

$$\Delta\mu = \Delta A A_2 = \Delta B B_2 = AB$$

On déduit :

$$\Delta A_2 = B$$

et

$$\Delta B_2 = A$$

ou

$$A_2 = \frac{B}{\Delta} = B_1$$

et

$$= \frac{A}{\Delta} = A_1.$$

Or on sait, d'après le résultat du numéro précédent, que $A_1 \wedge B_1 = 1$; donc on a :

$$A_2 \wedge B_2 = 1$$

Et :

Les quotients du P.P.C.M. de deux nombres par ces nombres sont premiers entre eux.

176. Distributivité du P.P.C.M. pour le P.G.C.D.

Soient trois nombres A, B, C et leurs ensembles de diviseurs primaires A′, B′, C′.

On a :

$$A' \cup (B' \cap C') = (A' \cup B') \cap (A' \cup C')$$

D'où :

$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C).$$

Et :

L'opération P.P.C.M. est distributive pour l'opération P.G.C.D.

177. Distributivité du P.G.C.D. pour le P.P.C.M.

Soient trois nombres A, B, C et leurs ensembles de diviseurs primaires A′, B′, C′.

On a :

$$A' \cap (B' \cup C') = (A' \cap B') \cup (A' \cap C')$$

D'où

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C).$$

Et :

L'opération P.G.C.D. est distributive pour l'opération P.P.C.M.

CHAPITRE XX

L'ANNEAU Z DES ENTIERS RATIONNELS

178. Relation d'équivalence dans N .

Soient $(\mathbf{a}'; \mathbf{b})$ ***et*** $(\mathbf{a}'; \mathbf{b}')$ ***deux éléments de l'ensemble-produit*** $N \times N = N^2$***. Ces deux éléments sont dits liés par la relation*** $\mathfrak{R}$ ***si*** $\mathbf{a} + \mathbf{b}' = \mathbf{b} + \mathbf{a}'$.

On note alors :

$$(a; b) = (a'; b'), \text{ mod } \mathfrak{R}.$$

Donc :

$$[(\mathbf{a};\mathbf{b}) = (\mathbf{a}';\mathbf{b}'), \textbf{mod}\,\mathfrak{R}] \quad \Leftrightarrow \quad (\mathbf{a} + \mathbf{b}' = \mathbf{b} + \mathbf{a}').$$

La relation $\mathfrak{R}$ *ainsi définie est une relation d'équivalence;* en effet, elle possède les propriétés suivantes :

Réflexivité.

$$(a; b) = (a; b) \text{ mod } \mathfrak{R}$$

car

$$a + b = b + a.$$

Symétrie.

$$[(a; b) = (a'; b'), \text{ mod } \mathfrak{R}] \quad \Rightarrow [(a'; b') = (a; b), \text{ mod } \mathfrak{R}]$$

car

$$a + b' = b + a' \Rightarrow \; a' + b = b' + a.$$

Transitivité.

$$\left[\text{ et } \begin{matrix} (a; b) = (a'; b'), \text{ mod } \mathfrak{R} \\ (a'; b') = (a''; b''), \text{ mod } \mathfrak{R} \end{matrix}\right] \Rightarrow [(a; b) = (a''; b''); \text{ mod } \mathfrak{R}]$$

car de

$$a + b' = b + a' \quad \text{et} \quad a' + b'' = b' + a''$$

on déduit :

$$a + b' + a' + b'' = b + a' + b' + a''$$

ou, puisque $a' + b'$ est régulier pour l'addition dans N,

$$a + b'' = b + a''$$

c'est-à-dire : $(a; b) = (a''; b''), \text{ mod } \mathfrak{R}.$

179. Remarque.

Les éléments $(a;\, b)$ et $(a + n;\, b + n)$, où $n \in \mathrm{N}$, sont équivalents car
$$a + (b + n) = b + (a + n).$$

180. Classes d'équivalence.

La relation précédente partage l'ensemble des éléments de $N \times N$ en classes d'équivalence.

Par exemple :
$$\{\ (4;2);\ (5;3);\ (6;4);\ \ldots;\ (125;123);\ \ldots\ \}$$
est une des classes d'équivalence, car
$$(4;\, 2) = (5;\, 3) = (6;\, 4) = \ldots = (125;\, 123) = \ldots, \text{ mod } \mathcal{R}.$$

Les classes d'équivalence sont appelées des entiers rationnels, ou des entiers relatifs.

L'ensemble des entiers relatifs est désigné par Z.

Donc :
$$\mathrm{Z} = \frac{\mathrm{N} \times \mathrm{N}}{\mathcal{R}}.$$

181. Formes canoniques.

On a, par exemple,
$$(5;\, 3) = (4;\, 2) = (3;\, 1) = (2;\, 0) \quad , \text{ mod } \mathcal{R}$$
$$(3;\, 4) = (2;\, 3) = (1;\, 2) = (0;\, 1) \quad , \text{ mod } \mathcal{R}$$
$$(4;\, 4) = (3;\, 3) = (2;\, 2) = (1;\, 1) = (0;\, 0), \text{ mod } \mathcal{R}$$

Les éléments $(2;\, 0)$, $(0;\, 1)$, $(0;\, 0)$ sont les formes canoniques des entiers relatifs déterminés par $(5;\, 3)$; $(3;\, 4)$; $(4;\, 4)$.

Un entier rationnel se met toujours sous l'une des formes canoniques suivantes :
$$(m;\, 0) \qquad (0;\, m) \qquad (0;\, 0).$$

182. Addition des couples de N^2.

Soient* (a; b) *et* (a′; b′) *deux éléments de N^2.

On définit leur somme par la formule :
$$\mathbf{(a;b) + (a';b') = (a + a';b + b').}$$

◇ *Exemples.*

$$(2; 3) + (1; 2) = (3; 5)$$
$$(3; 1) + (4; 7) = (7; 8).$$

183. Compatibilité de l'équivalence et de l'addition dans N^2.

Soient les éléments $(a; b)$ et $(a'; b')$ et leur somme $(a + a'; b + b')$; soient les éléments $(c; d)$ et $(c'; d')$ et leur somme $(c + c'; d + d')$.

On se propose de montrer que

$$\left[\begin{array}{l}(a; b) = (c; d), \text{ mod } \mathcal{R} \\ \text{et} \\ (a'; b') = (c'; d'), \text{ mod } \mathcal{R}\end{array}\right] \Rightarrow [(a + a'; b + b') = (c + c'; d + d'), \text{ mod } \mathcal{R}.]$$

En effet :

$$(a; b) = (c; d), \text{ mod } \mathcal{R} \Rightarrow a + d = b + c$$

et

$$(a'; b') = (c'; d'), \text{ mod } \mathcal{R} \Rightarrow a' + d' = b' + c'.$$

D'où, par addition :

$$a + a' + d + d' = b + b' + c + c'$$

ou

$$(a + a') + (d + d') = (b + b') + (c + c')$$

ce qui prouve que

$$(a + a' ; b + b') = (c + c' ; d + d'), \text{ mod } \mathcal{R}.$$

184. Addition des entiers rationnels.

Soient les entiers rationnels

$$\alpha = \text{Cl}\,(a; b) = \text{Cl}\,(c; d) \quad \text{si} \quad (a; b) = (c; d), \text{ mod } \mathcal{R}$$
$$\alpha' = \text{Cl}\,(a'; b') = \text{Cl}\,(c'; d') \quad \text{si} \quad (a'; b') = (c'; d'), \text{ mod } \mathcal{R}$$

Si

$$\alpha + \alpha' = \text{Cl}\,(a + a'; b + b'),$$

d'après le résultat obtenu au numéro précédent, on a aussi :

$$\alpha + \alpha' = \text{Cl}\,(c + c'; d + d')$$

puisque :

$$(a + a'; b + b') = (c + c'; d + d'), \text{ mod } \mathcal{R}.$$

Cela justifie la définition suivante :

Soient deux entiers rationnels α et α'; leur somme $\alpha + \alpha'$ est l'entier rationnel associé à la somme d'un élément quelconque de α et d'un élément quelconque de α'.

◇ *Exemple.*

Soient les entiers rationnels α et β. Si (3; 1) est un élément de α et (5; 9) un élément de β, on a :

$$\begin{aligned}\alpha + \beta &= \text{Cl}\,[(3;1) + (5;9)]\\ &= \text{Cl}\,(8;10)\\ &= \text{Cl}\,(0;2).\end{aligned}$$

D'autre part :

$$(3;1) = (2;0), \bmod \mathcal{R}$$

et

$$(5;9) = (0;4), \bmod \mathcal{R}.$$

Donc (2; 0) est un représentant de α, et (0; 4) un représentant de β. D'où :

$$\begin{aligned}\alpha + \beta &= \text{Cl}\,[(2;0) + (0;4)]\\ &= \text{Cl}\,[(2;4)]\\ &= \text{Cl}\,[0;2].\end{aligned}$$

185. Propriétés de l'addition des entiers rationnels.

L'addition des entiers rationnels possède les propriétés suivantes :

Commutativité.

Soient les entiers rationnels

$$\alpha = \text{Cl}\,(a;\, b) \quad \text{et} \quad \alpha' = \text{Cl}\,(a';\, b').$$

On a :

$$\alpha + \alpha' = \text{Cl}\,(a + a';\, b + b')$$

et

$$\alpha' + \alpha = \text{Cl}\,(a' + a;\, b' + b) = \text{Cl}\,(a + a';\, b + b').$$

Donc :

[C] $$(\forall \alpha)\ (\forall \alpha')\ \alpha + \alpha' = \alpha' + \alpha.$$

Et :

L'addition des entiers rationnels est commutative.

Associativité.

Soient les entiers rationnels

$$\alpha = \text{Cl}\,(a;\, b),\ \alpha' = \text{Cl}\,(a';\, b') \quad \text{et} \quad \alpha'' = \text{Cl}\,(a'';\, b'').$$

On a :

$$(\alpha + \alpha') + \alpha'' = \text{Cl}\,(a + a'; b + b') + \text{Cl}\,(a''; b'')$$
$$= \text{Cl}\,((a + a') + a''; (b + b') + b'')$$
$$= \text{Cl}\,(a + a' + a''; b + b' + b'')$$

et

$$\alpha + (\alpha' + \alpha'') = \text{Cl}\,(a; b) + \text{Cl}\,(a' + a''; b' + b'')$$
$$= \text{Cl}\,(a + (a' + a''); b + (b' + b''))$$
$$= \text{Cl}\,(a + a' + a''; b + b' + b'').$$

Donc :

[A] $(\forall\alpha)\,(\forall\alpha')\,(\forall\alpha'') \quad (\alpha + \alpha') + \alpha'' = \alpha + (\alpha' + \alpha'').$

Et :

L'addition des entiers rationnels est associative.

Existence d'un élément neutre.

Soient les entiers rationnels

$$\alpha = \text{Cl}\,(a; b) \quad \text{et} \quad e = \text{Cl}\,(0; 0)$$

On a :

$$\alpha + e = \text{Cl}\,(a + 0; b + 0)$$
$$= \text{Cl}\,(a; b)$$
$$= \alpha.$$

D'où, en tenant compte de la commutativité :

[N] $(\forall\alpha) \quad \alpha + e = e + \alpha = \alpha.$

Et :

L'entier rationnel* e = Cl (0; 0) *est neutre pour l'addition des entiers rationnels.

Au lieu de noter e = Cl (0; 0), on note e = 0, puisque la loi est notée additivement.

Le neutre est unique.

Z est symétrisé pour l'addition.

Soit l'entier rationnel

$$\alpha = \text{Cl}\,(a; b)$$

On considère :

$$\alpha' = \text{Cl}\,(b; a)$$

On a :

$$\alpha + \alpha' = \text{Cl}\,(a + b\,;\, b + a)$$
$$= \text{Cl}\,(0\,;0)$$
$$= 0.$$

D'où en tenant compte de la commutativité :

[S] $(\forall \alpha)\ (\exists \alpha')\qquad \alpha + \alpha' = \alpha' + \alpha = 0.$

Et :

Tous les entiers rationnels ont un symétrique pour l'addition.

α' est l'opposé de α; on le note $\alpha' = -\alpha$.
Le symétrique $\alpha' = -\alpha$ est unique.

186. Groupe additif.

On considère l'ensemble Z des entiers rationnels muni de la loi d'addition précédente. Les éléments de cet ensemble forment un groupe, parce que l'addition possède les trois propriétés suivantes :

[A] : elle est associative.

[N] : il existe un élément neutre pour l'addition.

[S] : tout entier rationnel a un opposé.

De plus :

[C] : l'addition est commutative.

D'où :

Les entiers rationnels forment un groupe additif commutatif.

On pose :

$$Z^* = Z - \{\,0\,\}.$$

187. Régularité.

Soient trois entiers rationnels α, β et μ.

On suppose que l'on a :

$$\alpha + \mu = \beta + \mu.$$

En ajoutant $-\mu$ aux deux membres de cette égalité, on obtient :

$$(\alpha + \mu) + (-\mu) = (\beta + \mu) + (-\mu)$$

ou

$$\alpha + [\mu + (-\mu)] = \beta + [\mu + (-\mu)] \quad \text{Associativité}$$

ou

$$\alpha + 0 = \beta + 0$$

ou

$$\alpha = \beta.$$

Donc :

$$(\forall\alpha)\ (\forall\beta)\ (\forall\mu) : \quad \alpha + \mu = \beta + \mu \Rightarrow \alpha = \beta.$$

Et :

Tous les entiers rationnels sont réguliers pour l'addition.

188. Soustraction.

Soient $\alpha \in Z$ ***et*** $\beta \in Z$.

Trouver un entier rationnel x tel que

$$\alpha = \beta + x$$

s'appelle soustraire β ***de*** α.

En ajoutant $-\beta$ aux deux membres de l'égalité précédente, on obtient :

$$\begin{aligned}(-\beta) + \alpha &= (-\beta) + \beta + x \\ &= 0 + x \\ &= x.\end{aligned}$$

Le nombre x cherché est donc

$$x = \alpha + (-\beta)$$

Et :

Pour soustraire un entier rationnel, on ajoute son opposé.

Le nombre x est la différence entre α et β. On le note :

$$x = \alpha - \beta.$$

D'où :

$$\alpha - \beta = \alpha + (-\beta).$$

189. Multiplication des couples de N^2.

Soient (a; b) et (a'; b') deux éléments de N^2.

On définit leur produit par la formule :

$$(a; b) \cdot (a'; b') = (aa' + bb'; ab' + ba').$$

◇ *Exemples.*

$$(2; 3) \cdot (1; 2) = (2 + 6; 4 + 3) = (8; 7)$$

$$(3; 1)\,(2; 5) = (6 + 5; 15 + 2) = (11; 17).$$

190. Compatibilité de l'équivalence et de la multplication dans N^2.

Soient les éléments $(a; b)$ et $(a'; b')$ et leur produit $(aa' + bb'; ab' + ba')$; soient les éléments $(c; d)$ et $(c'; d')$ et leur produit $(cc' + dd'; cd' + dc')$.

On se propose de montrer que

$$\begin{matrix} [(a;b) = (c;d), \bmod \mathcal{R} \\ \text{et} \quad (a';b') = (c';d'), \bmod \mathcal{R}] \end{matrix} \Rightarrow \begin{matrix} [(aa' + bb';ab' + ba') = \\ (cc' + dd';cd' + dc'), \bmod \mathcal{R}]. \end{matrix}$$

En effet :

$$(a; b) = (c; d), \bmod \mathcal{R} \Rightarrow a + d = b + c$$

et

$$(a'; b') = (c'; d'), \bmod \mathcal{R} \Rightarrow a' + d' = b' + c'.$$

D'ou :

$$\begin{cases} a'(a + d) = a'(b + c) \\ b'(b + c) = b'(a + d) \\ c(a' + d') = c(b' + c') \\ d(b' + c') = d(a' + d') \end{cases} \quad \text{ou} \quad \begin{cases} aa' + da' = ba' + ca' \\ bb' + cb' = ab' + db' \\ ca' + cd' = cb' + cc' \\ db' + dc' = da' + dd' \end{cases}$$

Par addition, on obtient :

$$(aa' + bb' + cd' + dc') + (da' + cb' + ca' + db') = (ab' + ba' + cc' + dd') + (da' + db' + ca' + cb')$$

ou

$$(aa' + bb') + (cd' + dc') = (ab' + ba') + (cc' + dd')$$

c'est-à-dire :

$$(aa' + bb'; ab' + ba') = (cc' + dd'; cd' + dc'), \bmod \mathcal{R}.$$

191. Multiplication des entiers rationnels.

Soient les entiers rationnels

$$\alpha = \text{Cl}\,(a; b) = \text{Cl}\,(c; d) \quad \text{si} \quad (a; b) = (c; d), \bmod \mathcal{R}$$

$$\alpha' = \text{Cl}\,(a'; b') = \text{Cl}\,(c'; d') \quad \text{si} \quad (a'; b') = (c'; d'), \bmod \mathcal{R}.$$

Si

$$\alpha\alpha' = \text{Cl}\,(aa' + bb'; ab' + ba')$$

d'après le résultat obtenu au numéro précédent, on a aussi :

$$\alpha\alpha' = \text{Cl}\,(cc' + dd'; cd' + dc')$$

puisque

$$(aa' + bb'; ab' + ba') = (cc' + dd'; cd' + dc'), \text{ mod } \mathcal{R}.$$

Cela justifie la définition suivante.

Soient deux entiers rationnels α et α'; leur produit $\alpha\alpha'$ est l'entier rationnel associé au produit d'un élément quelconque de α et d'un élément quelconque de α'.

◇ *Exemple.*

Soient les entiers rationnels α et β. Si (3; 1) est un élément de α et (2,5) un élément de β, on a :

$$\begin{aligned}\alpha \cdot \beta &= \text{Cl}\,[(3; 1) \cdot (2; 5)]\\ &= \text{Cl}\,[(11; 17]\\ &= \text{Cl}\,(0; 6).\end{aligned}$$

D'autre part :

$$(3; 1) = (2; 0), \text{ mod } \mathcal{R}$$

et

$$(2; 5) = (0; 3), \text{ mod } \mathcal{R}.$$

Par suite :

$$\begin{aligned}\alpha \cdot \beta &= \text{Cl}\,[(2; 0) . (0; 3)]\\ &= \text{Cl}\,(0; 6).\end{aligned}$$

192. Propriétés de la multiplication des entiers rationnels.

La multiplication des entiers rationnels possède les propriétés suivantes :

Commutativité.

Soient les entiers rationnels

$$\alpha = \text{Cl}\,(a; b) \quad \text{et} \quad \alpha' = \text{Cl}\,(a'; b').$$

On a :

$$\alpha \cdot \alpha' = \text{Cl}\,(aa' + bb'; ab' + ba')$$

et

$$\begin{aligned}\alpha' \cdot \alpha &= \text{Cl}\,(a'a + b'b; a'b + b'a)\\ &= \text{Cl}\,(aa' + bb'; ab' + ba').\end{aligned}$$

Donc :

C $\quad (\forall\alpha)\,(\forall\alpha') \quad \alpha \cdot \alpha' = \alpha' \cdot \alpha.$

Et :

La multiplication des entiers rationnels est commutative.

Associativité.

Soient les entiers rationnels :

$$\alpha = \text{Cl}\ (a;\ b),\quad \alpha' = \text{Cl}\ (a';\ b')\quad \text{et}\quad \alpha'' = \text{Cl}\ (a'';\ b'').$$

On a :

$$\begin{aligned}(\alpha \cdot \alpha')\ \alpha'' &= \text{Cl}\ (aa' + bb';\ ab' + ba') \cdot \text{Cl}\ (a'';\ b'')\\ &= \text{Cl}\ (aa'a'' + bb'a'' + ab'b'' + ba'b'';\\ &\qquad aa'b'' + bb'b'' + ab'a'' + ba'a'').\end{aligned}$$

et

$$\begin{aligned}\alpha \cdot (\alpha'\alpha'') &= \text{Cl}\ (a;\ b) \cdot \text{Cl}\ (a'a'' + b'b'';\ a'b'' + b'a'')\\ &= \text{Cl}\ (aa'a'' + ab'b'' + ba'b'' + bb'a'';\\ &\qquad aa'b'' + ab'a'' + ba'a'' + bb'b'').\end{aligned}$$

Les résultats sont identiques. Donc :

[A] $$(\forall\alpha)\ (\forall\alpha')\ (\forall\alpha'')\quad (\alpha \cdot \alpha')\ \alpha'' = \alpha\ (\alpha' \cdot \alpha'').$$

Et :

La multiplication des entiers rationnels est associative.

Existence d'un élément neutre.

Soient les entiers rationnels :

$$\alpha = \text{Cl}\ (a;\ b)\quad \text{et}\quad \varepsilon = \text{Cl}\ (1;\ 0).$$

On a :

$$\begin{aligned}\alpha \cdot \varepsilon &= \text{Cl}\ [(a;\ b) \cdot (1;\ 0)]\\ &= \text{Cl}\ (a;\ b)\\ &= \alpha.\end{aligned}$$

D'où, en tenant compte de la commutativité.

[N] $$(\forall\alpha)\quad \alpha \cdot \varepsilon = \varepsilon \cdot \alpha = \alpha.$$

Et :

L'entier rationnel $\varepsilon = \text{Cl}\ (1;\ 0)$ ***est neutre pour la multiplication des entiers rationnels.***

Au lieu de noter : $\varepsilon = \text{Cl}\ (1; 0)$, on note : $\varepsilon = 1$, puisque la loi est notée multiplicativement.

Ce neutre est unique.

193. Distributivité de la multiplication pour l'addition.

Soient les entiers rationnels :

$$\alpha = \text{Cl}\,(a;\, b) \quad \alpha' = \text{Cl}\,(a';\, b') \quad \text{et} \quad \mu = \text{Cl}\,(p;\, q)$$

On a :

$$\begin{aligned} \mu\,(\alpha + \alpha') &= \text{Cl}\,(p;\, q) \cdot \text{Cl}\,(a + a';\, b + b') \\ &= \text{Cl}\,(pa + pa' + qb + qb';\, pb + pb' + qa + qa') \end{aligned}$$

et

$$\begin{aligned} \mu\alpha + \mu\alpha' &= \text{Cl}\,[(p;\, q) \cdot (a;\, b)] + \text{Cl}\,[(p;\, q) \cdot (a';\, b')] \\ &= \text{Cl}\,(pa + qb;\, pb + qa) + \text{Cl}\,(pa' + qb';\, pb' + qa') \\ &= \text{Cl}\,(pa + qb + pa' + qb';\, pb + qa + pb' + qa'). \end{aligned}$$

Les résultats sont identiques; donc, en tenant compte de la commutativité :

$\boxed{D}$ $\quad (\forall\alpha)\,(\forall\alpha')\,(\forall\mu) \quad \mu(\alpha + \alpha') = \mu\alpha + \mu\alpha'$

$$(\alpha + \alpha')\,\mu = \alpha\mu + \alpha'\mu.$$

Et :

La multiplication des entiers rationnels est distributive pour l'addition des entiers rationnels.

194. L'anneau Z des entiers rationnels.

L'ensemble Z des entiers rationnels est muni d'une loi de composition interne, notée additivement et douant Z d'une structure de groupe commutatif, c'est-à-dire possédant les propriétés suivantes :

$\boxed{A}$ $\quad (\forall\alpha)\,(\forall\alpha')\,(\forall\alpha'') \qquad (\alpha + \alpha') + \alpha'' = \alpha + (\alpha' + \alpha'')$

$\boxed{N}$ $\quad (\forall\alpha) \qquad \alpha + 0 = 0 + \alpha = \alpha$

$\boxed{S}$ $\quad (\forall\alpha)\,(\exists\, -\alpha) \qquad \alpha + (-\alpha) = (-\alpha) + \alpha = 0.$

$\boxed{C}$ $\quad (\forall\alpha)\,(\forall\alpha') \qquad \alpha + \alpha' = \alpha' + \alpha.$

L'ensemble Z est muni d'une seconde loi de composition interne, notée multiplicativement et possédant les propriétés suivantes :

$\boxed{A}$ $\quad (\forall\alpha)\,(\forall\alpha')\,(\forall\alpha'') \qquad (\alpha \cdot \alpha')\,\alpha'' = \alpha \cdot (\alpha' \cdot \alpha'').$

$\boxed{N}$ $\quad (\forall\alpha) \qquad \alpha \cdot 1 = 1 \cdot \alpha = \alpha.$

$\boxed{C}$ $\quad (\forall\alpha)\,(\forall\alpha') \qquad \alpha \cdot \alpha' = \alpha' \cdot \alpha.$

De plus la multiplication est distributive pour l'addition :

D $(\forall\alpha)\ (\forall\alpha')\ (\forall\mu)$ $\mu(\alpha + \alpha') = \mu\alpha + \mu\alpha'$
$(\alpha + \alpha')\mu = \alpha\mu + \alpha'\mu.$

On traduit le fait que l'addition dans Z possède les propriétés A N S C, que la multiplication possède la propriété A et que l'addition et la multiplication sont liées par la propriété D, en disant que Z, muni des deux lois, a une structure d'anneau.

Comme la multiplication est aussi commutative, l'anneau est dit commutatif.

Comme la multiplication possède un élément neutre ou unité, l'anneau est dit unitaire.

En résumé :

Z est l'anneau commutatif unitaire des entiers rationnels.

195. Plongement de N dans Z.

Soit Z' l'ensemble des entiers rationnels de la forme Cl $(m; 0)$.

On peut envisager l'application φ qui à $m \in$ N fait correspondre Cl $(m; 0) \in$ Z' :

φ : $m \in \mathrm{N} \longrightarrow \varphi(m) = \mathrm{Cl}\,(m; 0) \in \mathrm{Z}'.$

Cette application est manifestement bijective.

De plus on a :

$$\varphi(m + m') = \mathrm{Cl}\,(m + m'; 0)$$
$$= \mathrm{Cl}\,(m; 0) + \mathrm{Cl}\,(m'; 0)$$

ou

$$\varphi(m + m') = \varphi(m) + \varphi(m')$$

et :

$$\varphi(mm') = \mathrm{Cl}\,(mm'; 0)$$
$$= \mathrm{Cl}\,(m; 0) \cdot \mathrm{Cl}\,(m'; 0)$$
$$= \varphi(m) \cdot \varphi(m').$$

On traduit ces deux résultats en disant que l'application φ respecte l'addition et la multiplication.

Il est donc possible d'identifier m et Cl $(m; 0)$, c'est-à-dire d'identifier N et Z'. On dit alors qu'on a plongé, ou immergé, N dans Z.

196. Entiers rationnels positifs. Entiers rationnels négatifs.

Les nombres entiers rationnels de la forme* Cl (m; *0*) *sont appelés des entiers positifs; ceux qui ont la forme* Cl (*0*; m) *sont appelés entiers négatifs.

On pose :

$$\text{Cl}\,(m; 0) = +m$$

et

$$\text{Cl}\,(0; m) = -m.$$

Les symboles + et — figurant ici font partie intégrante du nombre. Ce sont des *signes prédicatoires*, par opposition aux signes +, indiquant l'addition, et —, indiquant la soustraction, qui sont des signes opératoires.

Les nombres $+m$ et $-m$ sont opposés; ils ont des signes opposés.

L'ensemble des nombres positifs ou nul se note Z_+; Z_+ *contient* 0. *Si* $\alpha \in Z_+ - \{0\}$, *le nombre* α *est dit strictement positif.*

Z_- *représente l'ensemble des entiers négatifs (strictement négatifs).*

On pose :

$$Z_+^* = Z_+ - \{0\}.$$

197. Comparaison des entiers rationnels.

1° ***L'entier rationnel** α **est dit inférieur à** β**, si** $\alpha - \beta$ **est négatif.***

On écrit :

$$\alpha < \beta.$$

Et :

$$(\alpha < \beta) \Leftrightarrow (\alpha - \beta \in Z_-).$$

2° ***L'entier rationnel** α **est dit strictement supérieur à** β**, si** $\alpha - \beta$ **est strictement positif.***

$$\alpha > \beta.$$

Et :

$$(\alpha > \beta) \Leftrightarrow (\alpha - \beta \in Z_+^*).$$

3° ***Si** $\alpha \in Z_-$**,** α **est inférieur à 0.***

En effet :

$$(\alpha \in Z_-) \Leftrightarrow (\alpha - 0 \in Z_-) \Leftrightarrow (\alpha < 0).$$

De même :

$$(\alpha \in Z_+^*) \Leftrightarrow (\alpha > 0).$$

198. Valeur absolue d'un entier rationnel.

1° Soit $\alpha \in Z$. On définit une application de Z dans Z_+ par :

$$v: \quad \alpha = +m \longrightarrow v(\alpha) = +m$$

et

$$\alpha = -m \longrightarrow v(\alpha) = +m$$

$v(\alpha)$ *est la valeur absolue de* α; et on note :

$$v(\alpha) = |\alpha|.$$

Donc :

$$|\alpha| = \alpha \quad \textit{si} \quad \alpha \geqslant 0$$
$$|\alpha| = -\alpha \quad \textit{si} \quad \alpha < 0.$$

2° On a immédiatement les résultats suivants :

$$|-\alpha| = |\alpha|$$

et

$$|\alpha| = 0 \Leftrightarrow \alpha = 0.$$

3° Si $\alpha > 0$, on peut écrire : $\alpha = +|\alpha|$
Si $\alpha < 0$, on peut écrire : $\alpha = -|\alpha|$.

199. Les règles de l'addition.

1° Addition de deux nombres de même signe.

On a :

$$(+m) + (+n) = (m; 0) + (n; 0) = (m+n; 0) = +(m+n)$$

et

$$(-m) + (-n) = (0; m) + (0; n) = (0; m+n) = -(m+n).$$

Et :

La somme de deux nombres entiers rationnels de même signe est un nombre rationnel :
— dont le signe est le signe commun;
— dont la valeur absolue est la somme des valeurs absolues des deux nombres.

2° Addition de deux nombres de signes contraires.

On a, si $m > n$:

$$(+m) + (-n) = (m; 0) + (0; n) = (m; n) = (m-n; 0) = +(m-n)$$

et si $m < n$:

$$(+m) + (-n) = (m; 0) + (0; n) = (m; n) = (0; n-m) = -(n-m).$$

Et :

La somme de deux nombres entiers rationnels de signes contraires est un nombre entier rationnel :

— dont le signe est le signe du nombre qui a la plus grande valeur absolue;

— dont la valeur absolue est la différence des valeurs absolues des deux nombres.

3° *Si les deux nombres sont opposés* (m = n), *la somme est nulle.*

200. Valeurs absolues d'une somme et d'une différence.

1° Les règles précédentes permettent d'écrire :

$$\big||\alpha| - |\alpha'|\big| \leqslant |\alpha + \alpha'| \leqslant |\alpha| + |\alpha'|.$$

2° En remarquant que

$$\alpha - \alpha' = \alpha + (-\alpha')$$

on déduit de l'inégalité précédente :

$$\big||\alpha| - |\alpha'|\big| \leqslant |\alpha - \alpha'| \leqslant |\alpha| + |\alpha'|$$

201. Les règles de la multiplication.

On a :

$$(+m)\cdot(+n) = (m;0)\cdot(n;0) = (mn;0) = +(mn)$$
$$(-m)\cdot(-n) = (0;m)\cdot(0;n) = (mn;0) = +(mn)$$
$$(+m)\cdot(-n) = (m;0)\cdot(0;n) = (0;mn) = -(mn)$$
$$(-m)\cdot(+n) = (0;m)\cdot(n;0) = (0;mn) = -(mn)$$

Et :

Le produit de deux nombres entiers rationnels est un nombre entier rationnel

— dont le signe est le signe + si les deux nombres sont de même signe,

le signe — si les deux nombres ont des signes opposés,

— dont la valeur absolue est le produit des valeurs absolues des deux nombres.

202. Stabilité de Z_+.

Si α et β appartiennent à Z_+, la somme $\alpha + \beta$ et le produit $\alpha\beta$ de ces deux nombres appartiennent aussi à Z_+.

Donc :

Z_+ est une partie stable de Z par rapport à l'addition et à la multiplication.

203. Intégrité.

Soient α et β deux entiers rationnels. On a :

$$(\alpha\beta = 0) \Leftrightarrow |\alpha\beta| = 0 \Leftrightarrow |\alpha| \cdot |\beta| = 0 \Leftrightarrow (|\alpha| = 0 \text{ ou } |\beta| = 0)$$
$$\Leftrightarrow (\alpha = 0 \text{ ou } \beta = 0).$$

Donc :

Si le produit de deux entiers rationnels est nul alors l'un au moins de ces deux nombres est nul.

Autrement dit, dans Z il y a intégrité; et

Z est anneau commutatif unitaire et intègre.

204. Régularité.

Soient trois entiers rationnels α, β, μ avec $\mu \neq 0$.

On suppose que l'on a :

$$\alpha \cdot \mu = \beta \cdot \mu$$

D'où :

$$\alpha \cdot \mu - \beta \cdot \mu = 0$$

ou

$$\mu(\alpha - \beta) = 0$$

μ n'étant pas nul, d'après l'intégrité, on a :

$$\alpha - \beta = 0$$

ou

$$\alpha = \beta$$

Donc :

$$(\forall\alpha)(\forall\beta)(\forall\mu)\ (\alpha \in Z;\ \beta \in Z;\ \mu \in Z^*) : \quad \alpha\mu = \beta\mu \Rightarrow \alpha = \beta.$$

Et :

Tous les entiers rationnels non nuls sont réguliers pour la multiplication.

205. Eléments symétriques pour la multiplication.

Soient deux entiers rationnels α et α'.

Pour que α et α' soient symétriques pour la multiplication (c'est-à-dire inverses), il faut et il suffit que $\alpha\alpha' = 1$, donc que α et α' soient de même signe et que $|\alpha\alpha'| = 1$.

Or :

$$|\alpha\alpha'| = 1 \Leftrightarrow |\alpha| \cdot |\alpha'| = 1 \Leftrightarrow (|\alpha| = 1 \quad \text{et} \quad |\alpha'| = 1).$$

Donc :

$$\alpha = +1 \text{ a pour inverse } \alpha = +1$$

et

$$\alpha = -1 \text{ a pour inverse } \alpha = -1.$$

+ 1 et − 1 sont les seuls éléments inversibles de Z.

206. Ordre total.

La relation d'inégalité-égalité, notée $\leqslant$, est une relation d'ordre total.

En effet, cette relation possède les propriétés suivantes.

Réflexivité.

$$\alpha \leqslant \alpha$$

car :

$$\alpha - \alpha = 0.$$

Antisymétrie.

$$(\alpha \leqslant \beta \quad \text{et} \quad \beta \leqslant \alpha) \Rightarrow \alpha = \beta$$

car :

$$(\alpha - \beta \leqslant 0 \quad \text{et} \quad \beta - \alpha \leqslant 0) \Rightarrow \alpha - \beta = 0 \Rightarrow \alpha = \beta.$$

Transivité.

$$(\alpha \leqslant \beta \quad \text{et} \quad \beta \leqslant \gamma) \Rightarrow \alpha \leqslant \gamma$$

car de

$$\alpha - \beta \leqslant 0 \quad \text{et} \quad \beta - \gamma \leqslant 0$$

on tire :

$$\alpha - \beta + \beta - \gamma \leqslant 0$$

ou

$$\alpha - \gamma \leqslant 0$$

ou

$$\alpha \leqslant \gamma.$$

De plus, l'ordre est total, car deux entiers rationnels quelconques α et β sont comparables puisqu'on a $\alpha \leqslant \beta$ ou $\beta \leqslant \alpha$.

207. Addition et ordre.

Soient deux entiers α et β rationnels tels que :

$$\alpha \leqslant \beta$$

On a :

$$\alpha - \beta \leqslant 0$$

ou

$$\alpha + \gamma - \beta - \gamma \leqslant 0$$

ou

$$\alpha + \gamma \leqslant \beta + \gamma.$$

Donc :

$$(\alpha \leqslant \beta) \Rightarrow (\alpha + \gamma \leqslant \beta + \gamma).$$

Et :

L'addition dans Z est compatible avec l'ordre total dans Z.

208. Multiplication et ordre.

1° *Soit* μ *un nombre entier rationnel positif :* $\mu \in Z_+^*$.

Si $\alpha > \beta$ ou $\alpha - \beta > 0$, on a :

$$\mu(\alpha - \beta) > 0, \quad \text{ou} \quad \mu\alpha - \mu\beta > 0, \quad \text{ou} \quad \mu\alpha > \mu\beta$$

Donc :

$$(\mu > 0,\ \alpha > \beta) \Rightarrow (\mu\alpha > \mu\beta)$$

Si $\alpha < \beta$ ou $\alpha - \beta < 0$, on a :

$$\mu(\alpha - \beta) < 0, \quad \text{ou} \quad \mu\alpha - \mu\beta < 0, \quad \text{ou} \quad \mu\alpha < \mu\beta$$

Donc :

$$(\mu > 0,\ \alpha < \beta) \Rightarrow (\mu\alpha < \mu\beta).$$

D'où l'énoncé :

On peut multiplier les deux membres d'une inégalité de nombres entiers rationnels par un même nombre entier rationnel strictement positif sans changer le sens de cette inégalité.

2° *Soit* μ *un nombre entier rationnel négatif :* $\mu \in Z_-$.

Si $\alpha > \beta$ ou $\alpha - \beta > 0$, on a :

$$\mu(\alpha - \beta) < 0, \quad \text{ou} \quad \mu\alpha - \mu\beta < 0, \quad \text{ou} \quad \mu\alpha < \mu\beta$$

Donc :

$$(\mu < 0,\ \alpha > \beta) \Rightarrow (\mu\alpha < \mu\beta)$$

Si $\alpha < \beta$ ou $\alpha - \beta < 0$, on a :

$$\mu(\alpha - \beta) > 0, \quad \text{ou} \quad \mu\alpha - \mu\beta > 0, \quad \text{ou} \quad \mu\alpha > \mu\beta$$

Donc :

$$(\mu < 0,\ \alpha < \beta) \Rightarrow (\mu\alpha > \mu\beta).$$

D'où l'énoncé :

On peut multiplier les deux membres d'une inégalité de nombres entiers rationnels par un même nombre entier rationnel strictement négatif à condition de renverser le sens de l'inégalité.

3° *Les deux résultats précédents montrent que la multiplication dans Z n'est pas compatible avec l'ordre total dans Z.*

209. Conclusion.

L'ensemble Z a été muni d'une addition et d'une multiplication qui introduisent dans Z une structure d'anneau commutatif, unitaire et intègre.

La relation notée $\leqslant$ introduit un ordre total dans Z.

En conclusion :

L'ensemble Z des entiers rationnels est un anneau, commutatif, unitaire, intègre et totalement ordonné.

CHAPITRE XXI

CONGRUENCES DANS Z

210. Définition.

***Soient un nombre entier naturel* n *non nul* (n ∈ N*), *et deux nombres entiers rationnels* a *et* b (a ∈ Z; b ∈ Z).**

a *est dit congru à* b, *modulo* n, *s'il existe un entier rationnel* k (k ∈ Z) *tel que* a — b = k · n.

On note :

$$a = b, \text{ mod } n$$

et on a donc :

$$(\mathbf{a = b, \text{ mod } n}) \quad \Leftrightarrow \quad (\exists \mathbf{k})(\mathbf{k} \in Z) \; ; \quad \mathbf{a - b = kn}$$

et aussi :

$$(\mathbf{a = b, \text{ mod } n}) \quad \Leftrightarrow \quad (\exists \mathbf{k})(\mathbf{k} \in Z) : \quad \mathbf{a = b + kn.}$$

Lorsque $b = 0$, on obtient :

$$(\mathbf{a} = 0, \text{ mod } \mathbf{n}) \quad \Leftrightarrow \quad (\exists \mathbf{k})(\mathbf{k} \in Z) : \quad \mathbf{a = kn.}$$

211. Relation d'équivalence dans Z.

La relation binaire, définie au numéro précédent est bien une *relation d'équivalence* car elle possède les propriétés suivantes :

Réflexivité.

[R] $$(\forall a) \; a = a, \text{ mod } n.$$

En effet :

$$a = a + 0 \cdot n \quad \text{et} \quad k = 0.$$

Symétrie.

[S] $$(\forall a)(\forall b) \quad (a = b, \text{ mod } n) \quad \Rightarrow \quad (b = a, \text{ mod } n)$$

En effet :

$$a = b + k \cdot n \quad \Rightarrow \quad b = a + (-k) \cdot n$$

Transivité.

T $(\forall a)\,(\forall b)\,(\forall c)\ (a = b, \text{ mod } n \quad \text{et} \quad b = c, \text{ mod } n)$

$$\Rightarrow \quad (a = c;\ \text{mod } n).$$

En effet :

$$(a - b = kn \quad \text{et} \quad b - c = k'n) \Rightarrow a - c = (k + k')\,n$$

212. Classes d'équivalence.

La relation d'équivalence précédente partage Z en n classes d'équivalence.

***Ces classes d'équivalence sont les entiers modulo* n, *ou les classes résiduelles modulo* n.**

*L'ensemble de ces classes est noté Z/*n.

La classe de l'élément a *est noté* $\dot{a}$, *qui se lit « a point ».*

$$\text{Cl}\,(a) = \dot{a}.$$

◇ *Exemple 1.*

Si $n = 2$, on a deux classes :

$$\dot{0} = \{\ 0; 2; 4; 6; ...; -2; -4; -6; ...\ \}$$
$$\dot{1} = \{\ 1; 3; 5; 7; ...; -1; -3; -5; ...\ \}$$

Et alors :

$$Z/2 = \{\ \dot{0}\,;\dot{1}\ \}.$$

◇ *Exemple 2.*

Si $n = 5$, on a cinq classes :

$$\dot{0} = \{\ 0; 5; 10; 15; ...; -5; -10; -15; ...\ \}$$
$$\dot{1} = \{\ 1; 6; 11; 16; ...; -4; -\ 9; -14; ...\ \}$$
$$\dot{2} = \{\ 2; 7; 12; 17; ...; -3; -\ 8; -13; ...\ \}$$
$$\dot{3} = \{\ 3; 8; 13; 18; ...; -2; -\ 7; -12; ...\ \}$$
$$\dot{4} = \{\ 4; 9; 14; 19; ...; -1; -\ 6; -11; ...\ \}$$

Et alors :

$$Z/5 = \{\ \dot{0}\,;\dot{1}\,;\dot{2}\,;\dot{3}\,;\dot{4}\ \}.$$

Remarque.

Si on donne $a \in Z$ et la relation d'équivalence modulo n, la classe d'équivalence de a est l'ensemble $\dot{a}$ des nombres de la forme $a + kn$ ($k \in Z$).

$$\dot{a} = \{ x/x = a + kn,\ k \in Z \}.$$

213. Compatibilité de l'équivalence modulo n et de l'addition dans Z.

Soient les deux entiers rationnels a et b et leur somme $a + b$; soient encore les deux entiers rationnels a' et b' et leur somme $a' + b'$.

On se propose de démontrer l'implication :

$$(\mathbf{a}' = \mathbf{a},\ \mathbf{mod\ n\ et\ b}' = \mathbf{b},\ \mathbf{mod\ n}) \Rightarrow (\mathbf{a}' + \mathbf{b}' = \mathbf{a} + \mathbf{b},\ \mathbf{mod\ n})$$

En effet, on a :

$$a' = a + kn \qquad (k \in Z)$$
$$b' = b + k'n \qquad (k' \in Z)$$

D'où par addition :

$$a' + b' = a + b + (k + k')n \qquad (k + k' \in Z)$$

ou :

$$a' + b' = a + b, \text{ mod } n.$$

214. Addition des entiers modulo n.

Soient les entiers modulo n.

$$\alpha = \dot{a} = \dot{a}' \quad \text{si} \quad a' = a, \text{ mod } n$$
$$\beta = \dot{b} = \dot{b}' \quad \text{si} \quad b' = b, \text{ mod } n$$

Si

$$\alpha + \beta = \widehat{a + b},$$

d'après le résultat obtenu au numéro précédent, on a aussi :

$$\alpha + \beta = \widehat{a' + b'}$$

puisque :

$$(a' = a, \text{ mod } n \text{ et } b' = b, \text{ mod } n) \Rightarrow (a' + b' = a + b, \text{ mod } n).$$

Cela justifie la définition suivante :

***Soient deux entiers modulo* n, α *et* β*; leur somme* $\alpha + \beta$ *est l'entier modulo* n *associé à la somme d'un élément quelconque de* α *et d'un élément quelconque de* β.**

◇ *Exemple.*

Soient dans Z/5, les entiers modulo 5,

$$\alpha = \dot{2} \quad \text{et} \quad \beta = \dot{4}.$$

On a :

$$\alpha + \beta = \widehat{2 + 4}^{\,\cdot}$$
$$= \dot{1}$$

Donc :

$$\dot{2} + \dot{4} = \dot{1}.$$

215. Propriétés de l'addition.

L'addition des entiers modulo *n* possède les propriétés suivantes.

Commutativité.

Soient les entiers modulo *n*.

$$\alpha = \dot{a} \quad \text{et} \quad \alpha' = \dot{a}'$$

On a :

$$\alpha + \alpha' = \widehat{a + a'}^{\,\cdot}$$

et

$$\alpha' + \alpha = \widehat{a' + a}^{\,\cdot} = \widehat{a + a'}^{\,\cdot}.$$

Donc :

[C] $$(\forall\alpha)\,(\forall\alpha') : \quad \alpha + \alpha' = \alpha' + \alpha.$$

Et :

L'addition des entiers modulo n est commutative.

Associativité.

Soient les entiers modulo *n*.

$$\alpha = \dot{a}, \quad \alpha' = \dot{a}' \quad \text{et} \quad \alpha'' = \dot{a}''.$$

On a :

$$(\alpha + \alpha') + \alpha'' = \widehat{a + a'}^{\,\cdot} + \dot{a}''$$
$$= \widehat{a + a' + a''}^{\,\cdot}$$

et

$$\alpha + (\alpha' + \alpha'') = \dot{a} + \widehat{(a' + a'')}^{\,\cdot}$$
$$= \widehat{a + a' + a''}^{\,\cdot}.$$

Donc :

[A] $$(\forall\alpha)\,(\forall\alpha')\,(\forall\alpha'') : \quad (\alpha + \alpha') + \alpha'' = \alpha + (\alpha' + \alpha'').$$

Et :

L'addition des entiers modulo* n *est associative.

Existence d'un élément neutre.

Soient les entiers modulo n.

$$\alpha = \dot{a} \quad \text{et} \quad e = \dot{0}$$

On a :

$$\alpha + e = \widehat{a + 0}^{\,\cdot}$$
$$= \dot{a}$$

ou

$$\alpha + e = \alpha.$$

D'où, en tenant compte de la commutativité :

[N] $$(\forall\alpha) \quad \alpha + \dot{0} = \dot{0} + \alpha = \alpha.$$

Et :

***L'entier modulo* n e $= \dot{0}$ *est neutre pour l'addition des entiers modulo* n.**

Ce neutre est unique.

Z/*n *est symétrisé pour l'addition.

Soit l'entier modulo n :

$$\alpha = \dot{a}$$

On considère :

$$\alpha' = \widehat{n - a}^{\,\cdot}.$$

On a :

$$\alpha + \alpha' = \widehat{a + n - a}^{\,\cdot}$$
$$= \dot{n}$$
$$= \dot{0}$$

D'où, en tenant compte de la commutativité :

[S] $$(\forall\alpha)\,(\exists\alpha') : \quad \alpha + \alpha' = \alpha' + \alpha = \dot{0}.$$

Et :

Tous les entiers modulo* n *ont un symétrique pour l'addition.

α' est l'opposé de α; on peut le noter $\alpha' = -\alpha$.

Le symétrique $\alpha' = -\alpha$ est unique.

216. Groupe additif.

L'ensemble Z/n est donc muni d'une addition possédant les trois propriétés suivantes :

[A] $(\forall\alpha)\,(\forall\alpha')\,(\forall\alpha'')$ $\quad(\alpha + \alpha') + \alpha'' = \alpha + (\alpha' + \alpha'')$.

[N] $(\exists e)\,(e = \dot{0})\,(\forall\alpha)$ $\quad\alpha + \dot{0} = \dot{0} + \alpha = \alpha$.

[S] $(\forall\alpha)\,(\exists\alpha')$ $\quad\alpha + \alpha' = \alpha' + \alpha = \dot{0}$.

Z/n est donc un groupe. Comme de plus l'addition est commutative :

Les entiers modulo* n *forment un groupe additif commutatif.

On pose :

$$(Z/n)^* = Z/n - \{\dot{0}\}.$$

217. Régularité.

Soient les trois entiers modulo n : α, β et μ.

On suppose que l'on a :

$$\alpha + \mu = \beta + \mu.$$

En ajoutant $-\mu$ aux deux membres de cette égalité, on obtient :

$$(\alpha + \mu) + (-\mu) = (\beta + \mu) + (-\mu)$$

ou

$$\alpha + [\mu + (-\mu)] = \beta + [\mu + (-\mu)]$$

ou

$$\alpha + \dot{0} = \beta + \dot{0}$$
$$\alpha = \beta.$$

Donc :

$$(\forall\alpha)\,(\forall\beta)\,(\forall\mu) : \quad \alpha + \mu = \beta + \mu \Rightarrow \alpha = \beta.$$

Et :

Tous les entiers modulo* n *sont réguliers pour l'addition.

218. Soustraction.

Soient $\alpha \in Z/n$ et $\beta \in Z/n$.

Trouver un entier modulo n, x, *tel que*

$$\alpha = \beta + x$$

s'appelle soustraire β *de* α.

En ajoutant $-\beta$ aux deux membres de l'égalité précédente, on obtient :

$$\begin{aligned}(-\beta) + \alpha &= (-\beta) + \beta + x \\ &= \dot{0} + x \\ &= x\end{aligned}$$

Le nombre x cherché est donc :

$$x = \alpha + (-\beta)$$

Et :

Pour soustraire un entier modulo* n, *on ajoute son opposé.

Le nombre x est la différence entre α et β. On le note :

$$x = \alpha - \beta$$

D'où :

$$\alpha - \beta = \alpha + (-\beta).$$

219. Compatibilité de l'équivalence modulo *n* et de la multiplication dans Z.

Soient les deux entiers rationnels a et b et leur produit ab; soient encore les deux entiers rationnels a' et b', et leur produit $a'b'$.

On se propose de montrer que :

$$(\mathbf{a'} = \mathbf{a}, \bmod \mathbf{n} \quad \text{et} \quad \mathbf{b'} = \mathbf{b}, \bmod \mathbf{n}) \quad \Rightarrow \quad (\mathbf{a'b'} = \mathbf{ab}, \bmod \mathbf{n}).$$

En effet :

$$a' = a, \bmod n \Rightarrow a' = a + k \cdot n \qquad (k \in Z)$$

et :

$$b' = b, \bmod n \Rightarrow b' = b + k'n \qquad (k' \in Z)$$

D'où en multipliant :

$$\begin{aligned}a'b' &= ab + (kb + k'a + kk'n)n \\ &= ab + kn \qquad (k \in Z)\end{aligned}$$

ou :

$$a'b' = ab, \bmod n.$$

220. Multiplication des entiers modulo *n*.

Soient les entiers modulo n :

$$\alpha = \dot{a} = \dot{a}' \quad \text{si} \quad a' = a, \text{ mod } n$$

$$\beta = \dot{b} = \dot{b}' \quad \text{si} \quad b' = b, \text{ mod } n.$$

Si :

$$\alpha\beta = \dot{\widehat{ab}},$$

d'après le résultat obtenu au numéro précédent, on a aussi :

$$\alpha\beta = \dot{\widehat{a'b'}}$$

puisque :

$$(a' = a, \text{ mod } n \text{ et } b' = b, \text{ mod } n) \Rightarrow (a'b' = ab, \text{ mod } n).$$

Cela justifie la définition suivante :

***Soient deux entiers modulo* n, α *et* β*; leur produit* $\alpha\beta$ *est l'entier modulo* n *associé au produit d'un élément quelconque de* α *et d'un élément quelconque de* β.**

◇ *Exemple.*

Soient dans Z/5 les entiers relatifs

$$\alpha = \dot{2} \quad \text{et} \quad \beta = \dot{4}$$

On a :

$$\alpha\beta = \dot{\widehat{2 \times 4}}$$
$$= \dot{8}$$
$$= \dot{3}$$

Donc :

$$\dot{2} \times \dot{4} = \dot{3}.$$

221. Propriétés de la multiplication des entiers modulo *n*.

La multiplication des entiers modulo n possède les propriétés suivantes

Commutativité.

Soient les entiers modulo n :

$$\alpha = \dot{a} \quad \text{et} \quad \alpha' = \dot{a}'$$

On a :

$$\alpha\alpha' = \dot{\widehat{aa'}}$$

et

$$\alpha'\alpha = \dot{\widehat{a'a}}$$
$$= \dot{\widehat{aa'}}.$$

Donc :

C $$(\forall \alpha)\,(\forall \alpha') : \quad \alpha \cdot \alpha' = \alpha' \cdot \alpha.$$

Et :

La multiplication des entiers modulo n est commutative.

Associativité.

Soient les entiers modulo n :

$$\alpha = \dot{a}, \quad \alpha' = \dot{a}' \quad \text{et} \quad \alpha'' = \dot{a}''$$

On a :

$$(\alpha\alpha')\,\alpha'' = \dot{\widehat{aa'}} \cdot \dot{a}''$$
$$= \dot{\widehat{aa'a''}}$$

et

$$\alpha \cdot (\alpha'\alpha'') = \dot{a} \cdot \dot{\widehat{a'a''}}$$
$$= \dot{\widehat{aa'a''}}$$

Donc :

A $$(\forall \alpha)\,(\forall \alpha')\,(\forall \alpha'') : \quad (\alpha\alpha')\,\alpha'' = \alpha\,(\alpha'\alpha'').$$

Et :

La multiplication des entiers modulo n est associative.

Existence d'un élément neutre.

Soient les entiers modulo n :

$$\alpha = \dot{a} \quad \text{et} \quad \varepsilon = \dot{1}$$

On a :

$$\alpha \cdot \varepsilon = \dot{\widehat{a \times 1}}$$
$$= \dot{a}$$
$$= \alpha$$

D'où, en tenant compte de la commutativité :

N $$(\forall \alpha) \quad \alpha \cdot \dot{1} = \dot{1} \cdot \alpha = \alpha.$$

Et :

L'entier modulo n $\varepsilon = \dot{1}$ ***est neutre pour la multiplication des entiers modulo n.***

Ce neutre est unique.

222. Distributivité de la multiplication pour l'addition.

Soient les entiers modulo n :

$$\alpha = \dot{a} \quad \alpha' = \dot{a'} \quad \text{et} \quad \mu = \dot{m}$$

On a :

$$\mu(\alpha + \alpha') = \dot{m} \cdot \dot{\widehat{a + a'}}$$

$$= \dot{\widehat{m(a + a')}}$$

$$= \dot{\widehat{ma + ma'}}$$

et

$$\mu\alpha + \mu\alpha' = \dot{\widehat{ma}} + \dot{\widehat{ma'}}$$

$$= \dot{\widehat{ma + ma'}}.$$

Les résultats sont identiques; donc en tenant compte de la commutativité.

D $(\forall\alpha)\,(\forall\alpha')\,(\forall\mu)$: $\mu(\alpha + \alpha') = \mu\alpha + \mu\alpha'$

$(\alpha + \alpha')\,\mu = \alpha\mu + \alpha'\mu.$

Et :

La multiplication des entiers modulo n est distributive pour l'addition des entiers modulo n.

223. L'anneau Z/n des entiers modulo n.

L'ensemble Z/n des entiers modulo n est muni d'une loi de composition interne, notée additivement et douant Z/n d'une structure de groupe commutatif, c'est-à-dire possédant les propriétés suivantes :

A $(\forall\alpha)\,(\forall\alpha')\,(\forall\alpha'')$ $(\alpha + \alpha') + \alpha'' = \alpha + (\alpha' + \alpha'')$

N $(\forall\alpha)$ $\alpha + \dot{0} = \dot{0} + \alpha = \alpha$

S $(\forall\alpha)\,(\exists(-\alpha))$: $\alpha + (-\alpha) = (-\alpha) + \alpha = \dot{0}$

C $(\forall\alpha)\,(\forall\alpha')$ $\alpha + \alpha' = \alpha' + \alpha.$

L'ensemble Z/n est muni d'une seconde loi de composition interne, notée multiplicativement et possédant les propriétés suivantes :

[A] $(\forall\alpha)\ (\forall\alpha')\ (\forall\alpha'')$ $\quad (\alpha\alpha')\,\alpha'' = \alpha\,(\alpha'\alpha'')$

[N] $(\forall\alpha)$ $\quad \alpha\cdot\dot{1} = \dot{1}\cdot\alpha = \alpha$

[C] $(\forall\alpha)\ (\forall\alpha')$ $\quad \alpha\alpha' = \alpha'\alpha.$

De plus la multiplication est distributive pour l'addition :

[D] $(\forall\alpha)\ (\forall\alpha')\ (\forall\mu)$ $\quad \mu(\alpha + \alpha') = \mu\alpha + \mu\alpha'$
$\quad (\alpha + \alpha')\,\mu = \alpha\mu + \alpha'\mu.$

En conséquence :

L'ensemble Z/n est un anneau commutatif unitaire.

224. Etude de Z/2

$Z/2$ est formé de 2 entiers modulo 2 :

$\dot{0} = \{\ 0; 2; 4; 6; ...; -2; -4; -6; ...\ \}$
$\dot{1} = \{\ 1; 3; 5; 7; ...; -1; -3; -5; ...\ \}$

La table d'addition est :

$+$	$\dot{0}$	$\dot{1}$
$\dot{0}$	$\dot{0}$	$\dot{1}$
$\dot{1}$	$\dot{1}$	$\dot{0}$

et la table de multiplication est :

$\times$	$\dot{0}$	$\dot{1}$
$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$

225. Etude Z/3.

$Z/3$ est formé de 3 entiers modulo 3 :

$\dot{0} = \{\ 0; 3; 6; 9;\ ...; -3; -6; -9; ...\ \}$
$\dot{1} = \{\ 1; 4; 7; 10; ...; -2; -5; -8; ...\ \}$
$\dot{2} = \{\ 2; 5; 8; 11; ...; -1; -4; -7; ...\ \}$

La table d'addition est :

$+$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{0}$	$\dot{1}$

et la table de multiplication est :

$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{1}$

Si on envisage $(Z/3)^* = \{ \dot{1}; \dot{2} \}$, on voit que l'inverse de $\dot{1}$ est $\dot{1}$, et que l'inverse de $\dot{2}$ est $\dot{2}$.

Donc, les éléments de $(Z/3)^*$ ont un inverse.

Ainsi (Z/3) est muni d'une structure de groupe additif commutatif et (Z/3) est muni d'une structure de groupe multiplicatif commutatif; et de plus la multiplication est distributive pour l'addition.

Dans ces conditions on dit que :

Z/3 est un corps commutatif.

226. Etude de Z/5.

Z/5 est formé de 5 entiers modulo 5.

$\dot{0} = \{ 0; 5; 10; 15; ...; -5; -10; -15; ... \}$

$\dot{1} = \{ 1; 6; 11; 16; ...; -4; -9; -14; ... \}$

$$\dot{2} = \{ 2; 7; 12; 17; ...; -3; -8; -13; ... \}$$
$$\dot{3} = \{ 3; 8; 13; 18; ...; -2; -7; -12; ... \}$$
$$\dot{4} = \{ 4; 9; 14; 19; ...; -1; -6; -11; ... \}$$

On établit facilement la table d'addition :

+	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$

et la table de multiplication :

×	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{1}$	$\dot{3}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{1}$	$\dot{4}$	$\dot{2}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

Dans $(Z/5)^* = \{ \dot{1} ; \dot{2} ; \dot{3} ; \dot{4} \}$, l'inverse de $\dot{1}$ est $\dot{1}$

l'inverse de $\dot{2}$ est $\dot{3}$

l'inverse de $\dot{3}$ est $\dot{2}$

l'inverse de $\dot{4}$ est $\dot{4}$

Comme au numéro précédent, on a donc :

Z/5 est un corps commutatif.

227. Remarque.

De façon générale, on démontre le résultat suivant :

Si n est un nombre premier, Z/n est un corps commutatif.

228. Etude de Z/4.

Z/4 est formé de 4 entiers modulo 4.

$$\dot{0} = \{ 0; 4; 8; 12; ...; -4; -8; -12; ... \}$$
$$\dot{1} = \{ 1; 5; 9; 13; ...; -3; -7; -11; ... \}$$
$$\dot{2} = \{ 2; 6; 10; 14; ...; -2; -6; -10; ... \}$$
$$\dot{3} = \{ 3; 7; 11; 15; ...; -1; -5; -9; ... \}$$

On établit facilement la table d'addition :

$+$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{0}$	$\dot{1}$	$\dot{2}$

et la table de multiplication :

$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{0}$	$\dot{2}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

On voit ici que dans $(Z/4)^* = \{\dot{1}\,;\dot{2}\,;\dot{3}\}$, l'inverse de $\dot{1}$ est $\dot{1}$;
l'inverse de $\dot{3}$ est $\dot{3}$;

mais $\dot{2}$ n'a pas d'inverse. Donc Z/4 n'est pas un corps.

De plus, si le neutre pour l'addition $\dot{0}$ est appelé zéro, on voit ici que $\dot{2}\cdot\dot{2} = \dot{0}$. On traduit ce résultat en disant que $\dot{2}$ est un diviseur de zéro.

Donc :

Z/4 est un anneau commutatif unitaire avec un diviseur de zéro.

229. Etude de Z/6.

Z/6 est formé de 6 entiers modulo 6 :

$$\dot{0} = \{\ 0;\ \ 6;\ 12;\ 18;\ \dots;\ -6;\ -12;\ -18;\ \dots\ \}$$
$$\dot{1} = \{\ 1;\ \ 7;\ 13;\ 19;\ \dots;\ -5;\ -11;\ -17;\ \dots\ \}$$
$$\dot{2} = \{\ 2;\ \ 8;\ 14;\ 20;\ \dots;\ -4;\ -10;\ -16;\ \dots\ \}$$
$$\dot{3} = \{\ 3;\ \ 9;\ 15;\ 21;\ \dots;\ -3;\ -9;\ -15;\ \dots\ \}$$
$$\dot{4} = \{\ 4;\ 10;\ 16;\ 22;\ \dots;\ -2;\ -8;\ -14;\ \dots\ \}$$
$$\dot{5} = \{\ 5;\ 11;\ 17;\ 23;\ \dots;\ -1;\ -7;\ -13;\ \dots\ \}$$

On établit facilement la table d'addition :

$+$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{5}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$

et la table de multiplication :

$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{0}$	$\dot{2}$	$\dot{4}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{0}$	$\dot{3}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{2}$	$\dot{0}$	$\dot{4}$	$\dot{2}$
$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

Dans $(Z/6)^* = \{\dot{1} ; \dot{2} ; \dot{3} ; \dot{4} ; \dot{5}\}$, l'inverse de $\dot{1}$ est $\dot{1}$;
l'inverse de $\dot{5}$ est $\dot{5}$;

mais $\dot{2}$; $\dot{3}$; $\dot{4}$ ne sont pas inversibles.

De plus, on a : $\dot{2} \times \dot{3} = \dot{3} \times \dot{2} = \dot{0}$

$\dot{3} \times \dot{4} = \dot{4} \times \dot{3} = \dot{0}$.

Donc $\dot{2}$, $\dot{3}$, $\dot{4}$ sont des diviseurs de zéro, et :

Z/6 est un anneau commutatif unitaire avec diviseurs de zéro.

230. Remarque.

De façon générale on démontre le résultat suivant :

Si* n *n'est pas un nombre premier, Z/*n *est un anneau commutatif unitaire avec diviseurs de zéro.

231. Caractères de divisibilité.

Soit le nombre

$$A = \overline{u_n u_{n-1} \ldots u_1 u_0}$$
$$= u_n \cdot 10^n + u_{n-1} \cdot 10^{n-1} + \ldots + u_1 \cdot 10 + u_0.$$

1° Divisibilité par 2 ou par 5.

On a :

$$10 \equiv 0, \bmod 2$$

et

$$10 \equiv 0, \bmod 5$$

Donc : $A \equiv u_0, \bmod 2$

$\equiv u_0, \bmod 5$.

D'où :

Pour que le nombre A = $\overline{u_n u_{n-1} \ldots u_1 u_0}$ soit divisible par 2, il faut et il suffit que le chiffre des unités soit divisible par 2, c'est-à-dire que le nombre A soit terminé par 0, 2, 4, 6 ou 8.

Pour que le nombre A = $\overline{u_n u_{n-1} \ldots u_1 u_0}$ soit divisible par 5, il faut et il suffit que le chiffre des unités soit divisible par 5, c'est-à-dire que le nombre A soit terminé par 0 ou 5.

2° Divisibilité par 4 ou par 25.

On a :

$$100 \equiv 0, \bmod 4$$

et

$$100 \equiv 0, \bmod 25$$

comme

$$A = 100\,[u_n . 10^{n-2} + \cdots + u_2] + \overline{u_1 u_0}$$

On a : $A = \overline{u_1 u_0}$, mod 4

et

$A = \overline{u_1 u_0}$, mod 25.

D'où :

Pour que le nombre A = $\overline{u_n u_{n-1} \ldots u_1 u_0}$ soit divisible par 4, il faut et il suffit que le nombre formé par les deux derniers chiffres de droite soit divisible par 4.

Pour que le nombre A = $\overline{u_n u_{n-1} \ldots u_1 u_0}$ soit divisible par 25, il faut et il suffit que le nombre formé par les deux derniers chiffres de droite soit divisible par 25, c'est-à-dire que le nombre A soit terminé par 00, 25, 50 ou 75.

3° Divisibilité par 3 ou par 9.

On a :

$$10^n = 1, \text{ mod } 3$$

et

$$10^n = 1, \text{ mod } 9.$$

Par suite :

$$A = u_n + u_{n-1} + \ldots + u_1 + u_0, \text{ mod } 3$$

et

$$A = u_n + u_{n-1} + \ldots + u_1 + u_0, \text{ mod } 9.$$

D'où :

Pour le nombre A = $\overline{u_n u_{n-1} \ldots u_1 u_0}$ soit divisible par 3 (resp. par 9), il faut et il suffit que la somme de ses chiffres soit divisibles par 3 (resp. par 9).

4° Divisibilité par 11.

On a :

$$\begin{aligned} 10 &= -1, \text{ mod } 11 \\ 10^2 &= +1, \text{ mod } 11 \\ 10^3 &= -1, \text{ mod } 11 \\ 10^4 &= +1, \text{ mod } 11 \\ &\ldots\ldots\ldots \\ 10^n &= (-1)^n \text{ mod } 11 \end{aligned}$$

Donc :

$$A = u_0 - u_1 + u_2 - u_3 + \ldots + (-1)^n \cdot u_n, \text{ mod } 11.$$

D'où :

Pour que le nombre A = $u_n u_{n-1} \ldots u_1 u_0$ soit divisible par 11, il faut et il suffit que

$u_0 - u_1 + u_2 - u_3 + \ldots + (-1)^n u_n = 0$, mod 11,

c'est-à-dire que $u_0 - u_1 + u_2 - u_3 + \ldots + (-1)^n u_n$ soit divisible par 11.

CHAPITRE XXII

LE CORPS Q DES RATIONNELS

232. Relation d'équivalence dans $Z \times Z^*$.

***Soient** (a; b) **et** (a'; b') **deux éléments de l'ensemble-produit** $Z \times Z^*$.*

***Ces deux éléments sont dits liés par la relation** $\mathcal{R}$ **si** ab' = ba'.*

On note alors :

$$(a;b) = (a';b'), \text{ mod } \mathcal{R}.$$

Donc :

$$[(a;b) = (a';b'), \text{ mod } \mathcal{R}] \Leftrightarrow (ab' = ba').$$

La relation $\mathcal{R}$ ainsi définie est une *relation d'équivalence;* en effet, elle possède les propriétés suivantes :

Réflexivité.

$$(a;b) = (a;b), \text{ mod } \mathcal{R}$$

car $$ab = ba.$$

Symétrie.

$$[(a;b) = (a';b'), \text{ mod } \mathcal{R}] \Rightarrow [(a';b') = (a;b), \text{ mod } \mathcal{R}]$$

car $$ab' = ba' \Rightarrow a'b = b'a.$$

Transitivité.

$$[(a;b) = (a';b'), \text{ mod } \mathcal{R} \text{ et } (a';b') = (a'';b''), \text{ mod } \mathcal{R}] \Rightarrow [(a;b) = (a'';b''), \text{ mod } \mathcal{R}]$$

car de $$ab' = ba' \quad \text{et} \quad a'b'' = b'a''$$

on déduit : $$ab'a'b'' = ba'b'a''$$

ou, en simplifiant par $a'b'$:

$$ab'' = ba''$$

c'est-à-dire :

$$(a; b) = (a''; b''), \text{ mod } \mathcal{R}.$$

Cette démonstration suppose que a' n'est pas nul (car $b' \neq 0$). Lorsque a' est nul, $ab' = ba'$ implique $a = 0$, et $a'b'' = b'a''$ implique $a'' = 0$. Les trois éléments envisagés sont

$$(0; b) \quad (0; b') \quad (0; b'')$$

et par suite $(0; b)$ et $(0; b'')$ sont équivalents.

233. Notation $\frac{a}{b}$.

L'élément (a; b) *s'appelle fraction. Le nombre* a *est le numérateur; le nombre* b *est le dénominateur. Ce sont les deux termes de la fraction* (a; b).

Au lieu de noter $(a; b)$, on peut noter conformément à l'habitude $\frac{a}{b}$:

$$(a; b) = \frac{a}{b}.$$

234. Remarque.

Les fractions $(a; b)$ et $(na; nb)$, où $n \in Z^*$ sont équivalentes; en effet on a :

$$a \cdot nb = b \cdot na.$$

On peut alors écrire :

$$(a; b) = (na; nb), \text{ mod } \mathcal{R}$$

ou

$$\frac{a}{b} = \frac{na}{nb}.$$

235. Classes d'équivalence.

La relation d'équivalence modulo $\mathcal{R}$ précédente partage les éléments de $Z \times Z^*$ en classes d'équivalence.

Par exemple :

$$\{ (6; 12); (4; 8); (-13; -26); (-1; -2); (1; 2); \ldots \}$$

est une des classes d'équivalence.

Les classes d'équivalence portent le nom de nombres rationnels. L'ensemble des nombres rationnels est désigné par Q.

Donc :

$$Q = \frac{Z \times Z^*}{\mathfrak{R}}.$$

236. Formes canoniques.

1° ***Lorsque les nombres $|a|$ et $|b|$ sont premiers entre eux, la fraction (a; b) est dite forme canonique du nombre rationnel qu'elle définit.***

On dit aussi que le *nombre rationnel est réduit*, ou que *la fraction est irréductible.*

Par exemple les fractions :

$$(3; 7) \quad (-2; 11) \quad (1; -2)$$

sont irréductibles.

Il y a très souvent intérêt à utiliser les fractions irréductibles, car cela entraîne généralement une simplification des calculs.

2° La mise sous forme canonique s'appelle *simplification de la fraction.* Pour simplifier une fraction $(a; b)$ on en divise les deux termes par le P.G.C.D. de $|a|$ et $|b|$.

◇ *Exemple,*

Soit la fraction (7; 21). Le P.G.C.D. de 7 et 21 est 7. On a donc :

$$(7; 21) = (1; 3)$$

ou avec l'autre notation :

$$\frac{7}{21} = \frac{1}{3}.$$

237. Réduction au même dénominateur.

Deux fractions sont dites réduites au même dénominateur si leurs dénominateurs sont identiques.

Ainsi les fractions (3; 12) et (5; 12) sont réduites au même dénominateur.

Lorsqu'on veut réduire plusieurs fractions au même dénominateur, il y a souvent intérêt à prendre comme dénominateur commun le P.P.C.M. des dénominateurs.

◇ *Exemple.*

Réduire au même dénominateur les fractions (2; 3), (5; 6) et (2; 5).

Le P.P.C.M. des dénominateurs est 30. On a immédiatement :

$$(2; 3) = (20; 30) \qquad (5; 6) = (25; 30) \qquad (2; 5) = (12; 30)$$

ou avec l'autre notation :

$$\frac{2}{3} = \frac{20}{30} \qquad \frac{5}{6} = \frac{25}{30} \qquad \frac{2}{5} = \frac{12}{30}.$$

238. Addition des couples de Z × Z*.

Soient (a; b) et (a'; b') deux éléments de Z × Z*, c'est-à-dire deux fractions.

On définit leur somme par la formule

$$(\mathbf{a}; \mathbf{b}) + (\mathbf{a}'; \mathbf{b}') = (\mathbf{ab}' + \mathbf{ba}'; \mathbf{bb}')$$

ou avec l'autre notation :

$$\frac{\mathbf{a}}{\mathbf{b}} + \frac{\mathbf{a}'}{\mathbf{b}'} = \frac{\mathbf{ab}' + \mathbf{ba}'}{\mathbf{bb}'}.$$

◇ *Exemple 1.*

$$\begin{aligned}(2; 3) + (1; 4) &= (8 + 3; 12)\\ &= (11; 12)\end{aligned}$$

◇ *Exemple 2.*

$$\begin{aligned}(-4; 5) + (2; 3) &= (-12 + 10; 15)\\ &= (-2; 15)\end{aligned}$$

239. Compatibilité de l'équivalence et de l'addition dans Z × Z*.

Soient les fractions $(a; b)$ et $(a'; b')$, et leur somme $(ab' + ba'; bb')$; soient les éléments $(c; d)$ et $(c'; d')$, et leur somme $(cd' + dc'; dd')$.

On se propose de montrer que

$$\left[\text{et}\ \begin{matrix}(a; b) = (c; d), \text{ mod } \mathcal{R}\\ (a'; b') = (c'; d'), \text{ mod } \mathcal{R}\end{matrix}\right] \Rightarrow \left[\begin{matrix}(ab' + ba', bb') =\\ (cd' + dc'; dd'), \text{ mod } \mathcal{R}\end{matrix}\right]$$

En effet :

$$(a;\ b) = (c;\ d), \text{ mod } \mathcal{R} \Rightarrow \ ad = bc \ \text{ ou } \ ad - bc = 0$$

et

$$(a';\ b') = (c';\ d'), \text{ mod } \mathcal{R} \Rightarrow a'd' = b'c' \text{ ou } a'd' - b'c' = 0$$

D'où :

$$b'd'(ad - bc) + bd(a'd' - b'c') = 0$$

ou

$$adb'd' - bcb'd' + bda'd' - bdb'c' = 0$$

ou

$$dd'(ab' + ba') = bb'(cd' + dc')$$

ou

$$(ab' + ba'; bb') = (cd' + dc'; dd'), \bmod \mathcal{R}$$

240. Addition des rationnels.

Soient les rationnels :

$$\alpha = \text{Cl}(a;\ b) = \text{Cl}(c;\ d) \quad \text{si} \quad (a;\ b) = (c;\ d), \bmod \mathcal{R}$$
$$\alpha' = \text{Cl}(a';\ b') = \text{Cl}(c';\ d') \quad \text{si} \quad (a';\ b') = (c';\ d'), \bmod \mathcal{R}$$

Si

$$\alpha + \alpha' = \text{Cl}(ab' + ba';\ bb')$$

d'après le résultat obtenu au numéro précédent, on a aussi :

$$\alpha + \alpha' = \text{Cl}(cd' + dc';\ dd')$$

puisque :

$$(ab' + ba'; bb') = (cd' + dc'; dd'), \bmod \mathcal{R}.$$

Cela justifie la définition suivante :

Soient deux nombres rationnels α et α'; leur somme $\alpha + \alpha'$ est le nombre rationnel associé à la somme d'une fraction quelconque de α et d'une fraction quelconque de α'.

En particulier, on peut réduire les deux fractions choisies au même dénominateur. On obtient alors la règle classique d'addition :

$$(a; \delta) + (a'; \delta) = (a\delta + a'\delta; \delta^2)$$
$$= (a + a'; \delta)$$

ou avec l'autre notation:

$$\frac{\mathbf{a}}{\delta} + \frac{\mathbf{a}'}{\delta} = \frac{\mathbf{a} + \mathbf{a}'}{\delta}.$$

◇ *Exemple.*

Soient les rationnels :

$$\alpha = \text{Cl}(2; 3) \quad \text{et} \quad \alpha' = \text{Cl}(-1; 6)$$

En réduisant au même dénominateur :

$$\alpha = \text{Cl}(4; 6) \quad \text{et} \quad \alpha' = \text{Cl}(-1; 6)$$

D'où :

$$\alpha + \alpha' = \text{Cl}(4 - 1; 6)$$
$$= \text{Cl}(3; 6)$$
$$= \text{Cl}(1; 2)$$

241. Propriétés de l'addition des rationnels.

L'addition des nombres rationnels possède les propriétés suivantes :

Commutativité.

Soient les rationnels :

$$\alpha = \text{Cl}\,(a;\ b) \quad \text{et} \quad \alpha' = \text{Cl}\,(a';\ b')$$

On a :

$$\alpha + \alpha' = \text{Cl}\,(ab' + ba';\ bb')$$

et

$$\begin{aligned}\alpha' + \alpha &= \text{Cl}\,(a'b + b'a;\ b'b)\\ &= \text{Cl}\,(ab' + ba';\ bb')\end{aligned}$$

Donc :

$\boxed{C}$ $$(\forall\alpha)\ (\forall\alpha')\quad \alpha + \alpha' = \alpha' + \alpha.$$

Et :

L'addition des nombres rationnels est commutative.

Associativité.

Soient les rationnels, réduits au même dénominateur,

$$\alpha = \text{Cl}\,(a;\delta) \qquad \alpha' = \text{Cl}\,(a';\delta) \qquad \text{et} \qquad \alpha'' = \text{Cl}\,(a'';\delta)$$

On a :

$$\begin{aligned}(\alpha + \alpha') + \alpha'' &= \text{Cl}\,(a + a';\delta) + \text{Cl}(a'';\delta)\\ &= \text{Cl}\,(a + a' + a'';\delta)\end{aligned}$$

et

$$\begin{aligned}\alpha + (\alpha' + \alpha'') &= \text{Cl}\,(a;\delta) + \text{Cl}\,(a' + a'';\delta)\\ &= \text{Cl}\,(a + a' + a'';\delta)\end{aligned}$$

Donc :

$\boxed{A}$ $$(\forall\alpha)\ (\forall\alpha')\ (\forall\alpha'')\quad (\alpha + \alpha') + \alpha'' = \alpha + (\alpha' + \alpha'').$$

Et :

L'addition des nombres rationnels est associative.

Existence d'un élément neutre.

Soient les rationnels

$$\alpha = \text{Cl}(a;b) \quad \text{et} \quad e = \text{Cl}(0;1) = \text{Cl}(0;b)$$

On a :

$$\begin{aligned}\alpha + e &= \text{Cl}\,(a + 0;\ b)\\ &= \text{Cl}\,(a;\ b)\\ &= \alpha\end{aligned}$$

D'où en tenant compte de la commutativité :

N $(\exists e)\ (\forall \alpha) \quad \alpha + e = e + \alpha = \alpha.$

La loi étant additive, e est le zéro et on pose e $= 0$; on a alors :

N $(\forall \alpha) \quad \alpha + 0 = 0 + \alpha = \alpha.$

Q est symétrisé pour l'addition.

Soit le rationnel :

$$\alpha = \text{Cl}(a;\, b)$$

On considère :

$$\alpha' = \text{Cl}(-a;\, b)$$

On a :

$$\alpha + \alpha' = \text{Cl}(0;\, b) = 0.$$

D'où en tenant compte de la commutativité :

S $(\forall \alpha)\ (\exists \alpha') : \quad \alpha + \alpha' = \alpha' + \alpha.$

Et :

Tous les rationnels ont un symétrique pour l'addition.

α' est l'opposé de α; on le note $\alpha' = -\alpha$.

Le symétrique $\alpha' = -\alpha$ est unique.

242. Groupe additif.

On considère l'ensemble Q des rationnels muni de la loi d'addition précédente.

L'addition possède les propriétés suivantes :

A N S C

Donc :

Les nombres rationnels forment un groupe additif commutatif.

On pose : $\mathbf{Q}^* = \mathbf{Q} - \{ 0 \}.$

243. Régularité.

Soient trois rationnels α, β et μ.

On supppose que l'on a :

$$\alpha + \mu = \beta + \mu$$

En ajoutant $-\mu$ aux deux membres de cette égalité, on obtient :

$$(\alpha + \mu) + (-\mu) = (\beta + \mu) + (-\mu)$$

ou

$$\alpha + [\mu + (-\mu)] = \beta + [\mu + (-\mu)]$$

ou

$$\alpha + 0 = \beta + 0$$

ou

$$\alpha = \beta$$

Donc :

$$(\forall\alpha)\ (\forall\beta)\ (\forall\mu) : \quad \alpha + \mu = \beta + \mu \Rightarrow \alpha = \beta.$$

Et :

Tous les nombres rationnels sont réguliers pour l'addition.

244. Soustraction.

Soient $\alpha \in \mathbf{Q}$ ***et*** $\beta \in \mathbf{Q}$.
Trouver un rationnel x tel que

$$\alpha = \beta + \mathbf{x}$$

s'appelle soustraire β ***de*** α.

En ajoutant $-\beta$ aux deux membres de l'égalité précédente, on obtient :

$$\begin{aligned}(-\beta) + \alpha &= (-\beta) + \beta + x \\ &= 0 + x \\ &= x\end{aligned}$$

Le rationnel cherché est donc :

$$x = \alpha + (-\beta)$$

Et :

Pour soustraire un rationnel on ajoute son opposé.

Le nombre x est la différence entre α et β. On le note :

$$x = \alpha - \beta$$

D'où :

$$\alpha - \beta = \alpha + (-\beta)$$

245. Multiplication des couples de $\mathbf{Z} \times \mathbf{Z}^*$.

Soient (a; b) et (a'; b') deux fractions, c'est-à-dire deux éléments de $\mathbf{Z} \times \mathbf{Z}^*$.

On définit leur produit par la formule

$$(\mathbf{a}; \mathbf{b}) \cdot (\mathbf{a}'; \mathbf{b}') = (\mathbf{aa}'; \mathbf{bb}')$$

ou avec l'autre notation

$$\mathbf{\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}}.$$

◇ *Exemple 1.*

$$\begin{aligned}(2; 3) \cdot (1; 4) &= (2; 12)\\ &= (1; 6)\end{aligned}$$

◇ *Exemple 2.*

$$\begin{aligned}(-3; 5) \cdot (10; 2) &= (-30; 10)\\ &= (-3; 1)\end{aligned}$$

246. Compatibilité de l'équivalence et de la multiplication dans $\mathbf{Z} \times \mathbf{Z}^*$.

Soient les fractions $(a; b)$ et $(a'; b')$ et leur produit $(aa'; bb')$; soient les fractions $(c; d)$ et $(c'; d')$ et leur produit $(cc'; dd')$.

On se propose de montrer que

$$\left[\text{et}\ \begin{matrix}(a; b) = (c; d), \text{ mod } \mathcal{R}\\ (a'; b') = (c'; d'), \text{ mod } \mathcal{R}\end{matrix}\right] \Rightarrow \left[\begin{matrix}(aa'; bb') =\\ (cc'; dd'), \text{ mod } \mathcal{R}\end{matrix}\right]$$

En effet :

$$(a; b) = (c; d), \text{ mod } \mathcal{R} \Rightarrow ad = bc$$

et

$$(a'; b') = (c'; d'), \text{ mod } \mathcal{R} \Rightarrow a'd' = b'c'$$

D'où, par multiplication :

$$aa' \cdot dd' = bb' \cdot cc'$$

c'est-à-dire :

$$(aa'; bb') = (cc'; dd'), \text{ mod } \mathcal{R}.$$

247. Multiplication des rationnels.

Soient les nombres rationnels

$$\alpha = \text{Cl}(a; b) = \text{Cl}(c; d) \quad \text{si} \quad (a; b) = (c; d) \text{ mod } \mathcal{R}$$
$$\alpha' = \text{Cl}(a'; b') = \text{Cl}(c'; d') \quad \text{si} \quad (a'; b') = (c'; d'), \text{ mod } \mathcal{R}$$

Si

$$\alpha\alpha' = \text{Cl}(aa'; bb'),$$

d'après le résultat obtenu au numéro précédent, on a aussi :

$$\alpha\alpha' = \text{Cl}(cc'; dd')$$

puisque :

$$(aa'; bb') = (cc'; dd'), \text{ mod } \mathcal{R}$$

Cela justifie la définition suivante :

Soient deux rationnels α et α'; leur produit $\alpha\alpha'$ est le rationnel associé au produit d'une fraction quelconque de α et d'une fraction quelconque de α'.

248. Propriétés de la multiplication des rationnels.

La multiplication des nombres rationnels possède les propriétés suivantes.

Commutativité.

Soient les rationnels :

$$\alpha = \text{Cl}(a; b) \quad \text{et} \quad \alpha' = \text{Cl}(a'; b')$$

On a :

$$\alpha\alpha' = \text{Cl}(aa'; bb')$$

et

$$\alpha'\alpha = \text{Cl}(a'a; b'b) = \text{Cl}(aa'; bb')$$

Donc :

C $$(\forall\alpha)\,(\forall\alpha') \quad \alpha \cdot \alpha' = \alpha' \cdot \alpha.$$

Et :

La multiplication des rationnels est commutative.

Associativité.

Soient les rationnels :

$$\alpha = \text{Cl}(a; b) \qquad \alpha' = \text{Cl}(a'; b') \qquad \text{et} \qquad \alpha'' = \text{Cl}(a''; b'')$$

On a :

$$(\alpha\alpha')\alpha'' = \text{Cl}(aa'; bb') \times \text{Cl}(a''; b'') = \text{Cl}(aa'a''; bb'b'')$$

et

$$\alpha(\alpha'\alpha'') = \text{Cl}(a; b) \times \text{Cl}(a'a''; b'b'') = \text{Cl}(aa'a''; bb'b'')$$

Les résultats sont identiques. Donc :

A $$(\forall\alpha)\,(\forall\alpha')\,(\forall\alpha'') \quad (\alpha\alpha')\,\alpha'' = \alpha\,(\alpha'\alpha'').$$

Et :

La multiplication des rationnels est associative.

Existence d'un élément neutre.

Soient les rationnels :

$$\alpha = \text{Cl}(a;b) \qquad \text{et} \qquad \varepsilon = \text{Cl}(1;1)$$

On a :

$$\begin{aligned} \alpha \cdot \varepsilon &= \text{Cl}[a \times 1; b \times 1] \\ &= \text{Cl}(a;b) \\ &= \alpha \end{aligned}$$

D'où, en tenant compte de la commutativité :

[N] $$(\exists \varepsilon),\ \varepsilon = \text{Cl}(1;1),\ (\forall \alpha) \quad \alpha \cdot \varepsilon = \varepsilon \cdot \alpha = \alpha.$$

Et :

Le rationnel $\varepsilon =$ Cl (1; 1) est neutre pour la multiplication des rationnels.

Au lieu de noter $\varepsilon = \text{Cl}(1;1)$, on note $\varepsilon = 1$, puisque la loi est notée multiplicativement.

Le neutre est unique.

Q* est symétrisé pour la multiplication.

Soit le rationnel, non nul,

$$\alpha = \text{Cl}(a;b),$$

$\alpha \in Q^*$. On considère :

$$\alpha' = \text{Cl}(b;a)$$

On a :

$$\begin{aligned} \alpha\alpha' &= \text{Cl}(ab;ba) \\ &= \text{Cl}(1;1) \\ &= 1 \end{aligned}$$

D'où en tenant compte de la commutativité :

[S] $$(\forall \alpha)\ (\exists \alpha') \quad \alpha\alpha' = \alpha' \cdot \alpha = 1.$$

Et :

Tous les rationnels, non nuls, ont un symétrique pour la multiplication.

α' est l'inverse de α; on le note $\alpha' = \alpha^{-1}$.

L'inverse $\alpha' = \alpha^{-1}$ est unique.

249. Groupe multiplicatif.

L'ensemble $Q^* = Q - \{0\}$ est donc muni d'une multiplication possédant les trois propriétés suivantes :

[A] $(\forall\alpha)\,(\forall\alpha')\,(\forall\alpha'')$ $\quad (\alpha\alpha')\,\alpha'' = \alpha\,(\alpha'\alpha'')$.

[N] $(\forall\alpha)$ $\quad \alpha \times 1 = 1 \times \alpha = \alpha$.

[S] $(\forall\alpha)\,(\exists\alpha')$ $\quad \alpha\alpha' = \alpha'\alpha = 1$.

Q^* est donc un groupe. Comme de plus la multiplication est commutative :

Les rationnels non nuls forment un groupe multiplicatif commutatif.

250. Régularité.

Soient trois rationnels α, β et μ. $(\alpha \in Q;\ \beta \in Q;\ \mu \in Q^*)$.
On suppose que l'on a :

$$\alpha \cdot \mu = \beta \cdot \mu$$

En multipliant par $\mu' = \mu^{-1}$ les deux membres de cette égalité, on obtient :

$$(\alpha\mu)\,(\mu^{-1}) = (\beta\mu) \cdot \mu^{-1}$$

ou

$$\alpha \cdot (\mu \cdot \mu^{-1}) = \beta \cdot (\mu\mu^{-1})$$

ou

$$\alpha \times 1 = \beta \times 1$$

ou

$$\alpha = \beta.$$

Donc :

$(\forall\alpha)\,(\alpha \in Q),\ (\forall\beta)\,(\beta \in Q),\ (\forall\mu)\,(\mu \in Q^*)$: $\quad \alpha\mu = \beta\mu \Rightarrow \alpha = \beta$.

Et :

Tous les rationnels non nuls sont réguliers pour la multiplication.

251. Division.

Soient $\alpha \in \mathbf{Q}$ ***et*** $\beta \in \mathbf{Q}^*$.

Trouver un rationnel $\mathbf{x}$ ***(***$\mathbf{x} \in \mathbf{Q}$***) tel que***

$$\alpha = \beta \cdot \mathbf{x}$$

s'appelle diviser α ***par*** β.

En multipliant les deux membres de l'égalité précédente par $\beta' = \beta^{-1}$, on a :

$$\begin{aligned}\beta^{-1} \cdot \alpha &= \beta^{-1} (\beta x)\\ &= (\beta^{-1} \cdot \beta) x\\ &= 1 \cdot x\\ &= x.\end{aligned}$$

Le nombre x cherché est donc :

$$x = \alpha \cdot \beta^{-1}.$$

Et :

Pour diviser par un rationnel, non nul, on multiplie par son inverse.

252. Distributivité de la multiplication pour l'addition.

Soient les rationnels :

$$\alpha = \text{Cl}(a; \delta) \qquad \alpha' = \text{Cl}(a'; \delta) \qquad \text{et} \qquad \mu = \text{Cl}(p; q)$$

α et α' sont supposés réduits au même dénominateur.

On a :

$$\begin{aligned}\mu \cdot (\alpha + \alpha') &= \text{Cl}(p; q) \times \text{Cl}(a + a'; \delta)\\ &= \text{Cl}\ [p(a + a'); q\delta]\end{aligned}$$

et

$$\begin{aligned}\mu\alpha + \mu\alpha' &= \text{Cl}(p; q) \times \text{Cl}(a; \delta) + \text{Cl}(p; q) \times \text{Cl}(a'; \delta)\\ &= \text{Cl}(pa; q\delta) + \text{Cl}(pa'; q\delta)\\ &= \text{Cl}(pa + pa'; q\delta)\end{aligned}$$

Les résultats sont identiques; donc, en tenant compte de la commutativité :

D $\quad (\forall\alpha)\ (\forall\alpha')\ (\forall\mu) : \quad \mu(\alpha + \alpha') = \mu\alpha + \mu\alpha'$

$$(\alpha + \alpha')\mu = \alpha\mu + \alpha'\mu.$$

Et :

La multiplication des rationnels est distributive pour l'addition des rationnels.

253. Le corps Q des rationnels.

L'ensemble Q des rationnels est muni d'une loi de composition interne, notée additivement, et douant Q d'une structure de groupe commutatif, c'est-à-dire possédant les propriétés suivantes :

A $\quad (\forall\alpha)\ (\forall\alpha')\ (\forall\alpha'') : \quad (\alpha + \alpha') + \alpha'' = \alpha + (\alpha' + \alpha'').$

N $(\forall\alpha)$: $\alpha + 0 = 0 + \alpha = \alpha$

S $(\forall\alpha)\ (\exists(-\alpha))$: $\alpha + (-\alpha) = (-\alpha) + \alpha = 0$

C $(\forall\alpha)\ (\forall\alpha')$: $\alpha + \alpha' = \alpha' + \alpha.$

L'ensemble Q est muni d'une seconde loi de composition interne, notée multiplicativement, et douant Q* d'une structure de groupe commutatif, c'est-à-dire possédant les propriétés suivantes :

A $(\forall\alpha)\ (\forall\alpha')\ (\forall\alpha'')$: $(\alpha\alpha')\ \alpha'' = \alpha\ (\alpha'\alpha'').$

N $(\forall\alpha)$: $\alpha \times 1 = 1 \times \alpha = \alpha.$

S $(\forall\alpha)\ (\alpha \in Q^*)\ (\exists\alpha^{-1})$: $\alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = 1.$

C $(\forall\alpha)\ (\forall\alpha')$: $\alpha\alpha' = \alpha'\alpha.$

De plus la multiplication est distributive pour l'addition :

D $(\forall\alpha)\ (\forall\alpha')\ (\forall\mu)$: $\mu(\alpha + \alpha') = \mu\alpha + \mu\alpha'$
$(\alpha + \alpha')\,\mu = \alpha\mu + \alpha'\mu.$

On traduit le fait que l'addition dans Q possède les propriétés A N S C que la multiplication possède les propriétés A N S et que l'addition et la multiplication sont liées par la propriété D, en disant que Q, muni de ces deux lois, a une structure de corps.

Comme la multiplication est aussi commutative :

Q est le corps commutatif des rationnels.

254. Plongement de Z dans Q.

Soit Q' l'ensemble des rationnels de la forme $\text{Cl}\,(m; 1)$.

On peut envisager l'application φ qui à $m \in Z$ fait correspondre

$$\text{Cl}\,(m; 1) \in Q' :$$

$$\varphi : \quad m \in Z \longrightarrow \varphi\,(m) = \text{Cl}\,(m; 1) \in Q'.$$

Cette application est manifestement bijective.

De plus, on a :

$$\varphi(m + m') = \text{Cl}(m + m'; 1) = \text{Cl}(m; 1) + \text{Cl}(m'; 1)$$

ou

$$\varphi(m + m') = \varphi(m) + \varphi(m')$$

et :

$$\begin{aligned}\varphi(mm') &= \mathrm{Cl}(mm'; 1)\\ &= \mathrm{Cl}(m; 1) \times \mathrm{Cl}(m'; 1)\end{aligned}$$

ou

$$\varphi(mm') = \varphi(m) \cdot \varphi(m').$$

Et :

L'application φ respecte l'addition et la multiplication.

Il est donc possible d'identifier m et $\mathrm{Cl}(m; 1)$, c'est-à-dire d'identifier Z et Q'. On a alors plongé, ou immergé, Z dans Q.

Ainsi :

L'anneau Z est une partie du corps Q des rationnels.

Cela justifie le nom d'entier rationnel donné aux éléments de Z.

On a :

$$N \subset Z \subset Q.$$

255. Rationnels positifs. Rationnels négatifs.

1° De :

$$(a; b) = (a'; b'), \text{ mod } \mathcal{R}$$

on déduit :

$$ab' = ba'$$

et

$$ab' \cdot ba' = (ab')^2$$

ou

$$(ab) \cdot (a'b') = (ab')^2.$$

Donc les produits ab et $a'b'$ sont de même signe.

Et :

Si deux fractions (a; b) *et* (a'; b') *sont équivalentes, alors les produits* ab *et* a'b' *sont de même signe.*

2° Cette remarque justifie la définition suivante :

Soit le rationnel α **= Cl (a; b).**

Si le produit* ab *est positif, le rationnel α ***est dit positif.***

Si le produit* ab *est négatif, le rationnel α ***est dit négatif.***

3° *L'ensemble des nombres rationnels positifs se note* Q_+. Q_+ *contient 0. On pose :*

$$Q_+^* = Q_+ - \{0\}$$

Les éléments de Q_+^* sont les rationnels strictement positifs.
On représente par Q_- l'ensemble des rationnels strictement négatifs.

4° Soient $\alpha = \text{Cl}(a; b)$ et $-\alpha = \text{Cl}(-a; b)$. Ces deux nombres ont des signes opposés :

Un nombre et son opposé ont des signes opposés.

5° Soient $\alpha = \text{Cl}(a; b)$ et $\alpha^{-1} = \text{Cl}(b; a)$. Ces deux nombres sont de même signe, car ab et ba sont de même signe.

Un nombre et son inverse sont de même signe.

6° *Soit le rationnel* $\alpha = \text{Cl}(a; b)$. *On peut supposer* b *positif. Alors* α *et* a *sont de même signe.*

256. Comparaison des rationnels.

1° ***Le nombre rationnel*** α ***est dit inférieur à*** β ***si*** $\alpha - \beta$ ***est négatif.***

On écrit :

$$\alpha < \beta$$

Et :

$$(\alpha < \beta) \iff (\alpha - \beta \in Q_-).$$

2° ***Le nombre rationnel*** α ***est dit strictement supérieur à*** β ***si*** $\alpha - \beta$ ***est strictement positif.***

On écrit :

$$\alpha > \beta.$$

Et :

$$(\alpha > \beta) \iff (\alpha - \beta \in Q_+^*).$$

3° ***Si*** $\alpha \in Q_-$, α ***est inférieur à 0.***

En effet :

$$(\alpha \in Q_-) \iff (\alpha - 0 \in Q_-) \iff (\alpha < 0).$$

De même :

$$(\alpha \in Q_+^*) \iff (\alpha > 0).$$

257. Valeur absolue d'un rationnel.

1° Soit $\alpha \in Q$. On définit une application de Q dans Q_+ par

$$v : \quad \begin{aligned} \alpha &\longrightarrow v(\alpha) = \alpha, && \text{si } \alpha \geqslant 0 \\ \alpha &\longrightarrow v(\alpha) = -\alpha, && \text{si } \alpha < 0. \end{aligned}$$

$v(\alpha)$ est la valeur absolue de α; on note : $v(\alpha) = |\alpha|$

Donc :

$$|\alpha| = \alpha, \quad \textit{si} \quad \alpha \geqslant 0$$
$$|\alpha| = -\alpha, \quad \textit{si} \quad \alpha < 0.$$

2° On a immédiatement les résultats suivants :

$$|-\alpha| = |\alpha|$$

et

$$|\alpha| = 0 \iff \alpha = 0.$$

3° *Si* $\alpha > 0$, *on peut écrire :* $\alpha = +|\alpha|$
Si $\alpha < 0$, *on peut écrire :* $\alpha = -|\alpha|$

Ainsi le nombre rationnel α est l'ensemble d'un signe et d'une valeur absolue. Les signes + ou — font partie du nombre; ce sont des signes prédicatoires.

258. Les règles de l'addition.

Soient deux nombres rationnels :

$$\alpha = \text{Cl}(a; \delta) \quad \text{et} \quad \alpha' = \text{Cl}(a'; \delta)$$

réduits au même dénominateur positif δ.

On a :

$$\alpha + \alpha' = \text{Cl}(a + a'; \delta).$$

1° Le signe de $\alpha + \alpha'$ est celui de $a + a'$ puisque δ est positif. Donc :

Si α et α' sont de même signe, a et a' sont de même signe, et $\alpha + \alpha'$ a le signe de α et de α'.

Si α et α' ont des signes opposés, a et a' ont des signes opposés, et $a + a'$ a le signe du nombre qui a la plus grande valeur absolue, et $\alpha + \alpha'$ a le signe du nombre qui a la plus grande valeur absolue.

2° De plus;

$$|\alpha + \alpha'| = \text{Cl}(|a + a'|; \delta)$$

Donc :

Si α et α' sont de même signe : $|\alpha + \alpha'| = |\alpha| + |\alpha'|$

Si α et α' ont des signes opposés : $|\alpha + \alpha'| = \big||\alpha| - |\alpha'|\big|$

3° On a donc, comme pour l'addition dans Z,

La somme de deux nombres rationnels de même signe est un nombre rationnel

— dont le signe est le signe commun;

— dont la valeur absolue est la somme des valeurs absolues des deux nombres.

La somme de deux nombres rationnels de signes opposés est un nombre rationnel

— dont le signe est le signe du nombre qui a la plus grande valeur absolue;

— dont la valeur absolue est le différence des valeurs absolues des deux nombres.

259. Valeurs absolues d'une somme et d'une différence.

Comme dans Z (cf. nº 200) on a les inégalités suivantes :

$$\big||\alpha| - |\alpha'|\big| \leqslant |\alpha + \alpha'| \leqslant |\alpha| + |\alpha'|$$

et

$$\big||\alpha| - |\alpha'|\big| \leqslant |\alpha - \alpha'| \leqslant |\alpha| + |\alpha'|.$$

260. Les règles de la multiplication.

Soient deux rationnels, dont on peut supposer les dénominateurs positifs :

$$\alpha = \mathrm{Cl}(a; b) \quad \text{et} \quad \alpha' = \mathrm{Cl}(a'; b')$$

et leur produit :

$$\alpha\alpha' = \mathrm{Cl}(aa'; bb')$$

Le produit bb' étant positif, $\alpha\alpha'$ a le signe de aa'.

De plus :

$$\begin{aligned} |\alpha\alpha'| &= \mathrm{Cl}(|aa'|; bb') \\ &= \mathrm{Cl}(|a| \cdot |a'|; bb') \\ &= \mathrm{Cl}(|a|; b) \times \mathrm{Cl}(|a'|; b') \end{aligned}$$

ou

$$|\alpha\alpha'| = |\alpha| \cdot |\alpha'|$$

On a donc, comme pour la multiplication dans Z.

Le produit de deux rationnels est un rationnel

— dont le signe est le signe + si les deux nombres sont de même signe, le signe — si les deux nombres ont des signes opposés;

— dont la valeur absolue est le produit des valeurs absolues des deux nombres.

261. Stabilité de Q_+.

Si α et β appartiennent à Q_+, la somme $\alpha + \beta$ et le produit $\alpha\beta$ de ces deux nombres appartiennent aussi à Q_+.

Donc :

Q_+ est une partie stable de Q par rapport à l'addition et à la multiplication.

262. Relation d'ordre total.

La relation d'inégalité-égalité, notée $\leqslant$, est une relation d'ordre total.

En effet cette relation possède les propriétés suivantes :

Réflexivité :

$$\alpha \leqslant \alpha;$$

car

$$\alpha - \alpha = 0.$$

Antisymétrie :

$$(\alpha \leqslant \beta \text{ et } \beta \leqslant \alpha) \Rightarrow \alpha = \beta;$$

car

$$(\alpha - \beta \leqslant 0 \text{ et } \beta - \alpha \leqslant 0) \Rightarrow \alpha - \beta = 0 \Rightarrow \alpha = \beta.$$

Transitivité :

$$(\alpha \leqslant \beta \quad \text{et} \quad \beta \leqslant \gamma) \Rightarrow \alpha \leqslant \gamma;$$

car de

$$\alpha - \beta \leqslant 0 \quad \text{et} \quad \beta - \gamma \leqslant 0$$

on tire :

$$\alpha - \beta + \beta - \gamma \leqslant 0$$

ou

$$\alpha - \gamma \leqslant 0,$$

ou

$$\alpha \leqslant \gamma.$$

De plus, l'ordre est total, car deux nombres rationnels quelconques α et β sont comparables puisqu'on a $\alpha \leqslant \beta$ ou $\beta \leqslant \alpha$.

263. Addition et ordre.

Soient deux rationnels α et β tels que :

$$\alpha \leqslant \beta.$$

On a :

$$\alpha - \beta \leqslant 0$$

ou

$$\alpha + \gamma - \beta - \gamma \leqslant 0$$

ou

$$\alpha + \gamma \leqslant \beta + \gamma.$$

Donc :

$$(\alpha \leqslant \beta) \Rightarrow (\alpha + \gamma \leqslant \beta + \gamma).$$

Et :

L'addition dans Q est compatible avec l'ordre total dans Q.

264. Multiplication et ordre.

1° Soit μ un rationnel positif : $\mu \in Q^*_+$.

Si $\alpha > \beta$ ou $\alpha - \beta > 0$, on a :

$$\mu(\alpha - \beta) > 0 \quad \text{ou} \quad \mu\alpha - \mu\beta > 0 \quad \text{ou} \quad \mu\alpha > \alpha\beta.$$

Donc :

$$(\mu > 0 ; \alpha > \beta) \Rightarrow (\mu\alpha > \mu\beta).$$

Si $\alpha < \beta$ ou $\alpha - \beta < 0$, on a :

$$\mu(\alpha - \beta) < 0 \quad \text{ou} \quad \mu\alpha - \mu\beta < 0 \quad \text{ou} \quad \mu\alpha < \mu\beta.$$

Donc :

$$(\mu > 0 ; \alpha < \beta) \Rightarrow (\mu\alpha < \mu\beta).$$

D'où l'énoncé :

On peut multiplier les deux membres d'une inégalité de nombres rationnels par un même nombre rationnel strictement positif sans changer le sens de cette inégalité.

2° Soit μ un rationnel négatif : $\mu \in Q_-$.

Si $\alpha > \beta$ ou $\alpha - \beta > 0$, on a :

$$\mu(\alpha - \beta) < 0 \quad \text{ou} \quad \mu\alpha - \mu\beta < 0 \quad \text{ou} \quad \mu\alpha < \mu\beta.$$

Donc :

$$(\mu < 0 ; \alpha > \beta) \Rightarrow (\mu\alpha < \mu\beta).$$

Si $\alpha < \beta$ ou $\alpha - \beta < 0$, on a :

$$\mu(\alpha - \beta) > 0 \quad \text{ou} \quad \mu\alpha - \mu\beta > 0 \quad \text{ou} \quad \mu\alpha > \mu\beta$$

Donc :

$$(\mu < 0 ; \alpha < \beta) \quad \Rightarrow \quad (\mu\alpha > \mu\beta)$$

D'où l'énoncé :

On peut multiplier les deux membres d'une inégalité de nombres rationnels par un même nombre rationnel négatif à condition de renverser le sens de l'inégalité.

3º *Les deux résultats précédents montrent que la multiplication dans Q n'est pas compatible avec l'ordre total dans Q.*

265. Le corps Q est archimédien.

Soient α et β deux rationnels positifs quelconques, avec

$$0 < \alpha < \beta.$$

Dire que Q est un corps archimédien, c'est-à-dire qu'il existe un nombre entier naturel n, (n ∈ N) tel que

$$n\alpha > \beta.$$

En effet, en multipliant cette inégalité par α^{-1}, qui est positif comme α, on obtient $n > \beta \cdot \alpha^{-1}$.

Il suffit donc de prendre n supérieur à $\beta \cdot \alpha^{-1}$.

266. Le corps Q est divisible.

Soient α et β deux rationnels quelconques avec

$$\alpha < \beta.$$

Dire que Q est un corps divisible, c'est dire qu'entre les deux rationnels α et β, il existe au moins un autre rationnel.

En effet de $\alpha < \beta$ on déduit :

$$\alpha + \beta < 2\beta$$

et

$$2\alpha < \alpha + \beta$$

c'est-à-dire :

$$2\alpha < \alpha + \beta < 2\beta.$$

D'où :

$$\alpha < \frac{\alpha + \beta}{2} < \beta.$$

Le nombre $\frac{\alpha + \beta}{2}$ est rationnel et est compris entre α et β.

267. Conclusion.

L'ensemble Q a été muni d'une addition et d'une multiplication qui introduisent dans Q une structure de corps commutatif.

La relation notée $\leqslant$ est une relation d'ordre total.

En conclusion :

L'ensemble Q des nombres rationnels est un corps commutatif, totalement ordonné, archimédien et divisible.

268. Carré d'un nombre rationnel.

1° Soit un nombre rationnel représenté par la fraction irréductible $\frac{a}{b}$; son carré est un rationnel représenté par la fraction $\frac{a^2}{b^2}$.

Puisque a et b sont premiers entre eux, il en est de même de a^2 et b^2; donc la fraction $\frac{a^2}{b^2}$ est irréductible.

Et :

Le carré d'une fraction irréductible est une fraction irréductible.

2° Pour que $\frac{a^2}{b^2}$ soit un entier rationnel il faut et il suffit que $b^2 = 1$, c'est-à-dire que $b = +1$, donc que $\frac{a}{b}$ soit un entier rationnel.

Pour que le carré d'un rationnel soit un entier rationnel, il faut et il suffit que ce rationnel soit lui-même un entier rationnel.

3° Par suite :

Le carré d'un nombre rationnel, non entier rationnel, n'est jamais un entier rationnel.

Par exemple, il n'existe aucun entier rationnel dont le carré est 2. Une nouvelle extension de la notion de nombre est donc indispensable.

CHAPITRE XXIII

FRACTIONS DÉCIMALES

269. Fractions décimales.

On appelle fraction décimale une fraction dont le dénominateur est une puissance de 10.

◇ *Exemples.*

$$\frac{51}{10};\ \frac{4}{100};\ \frac{8345}{1\,000} \text{ sont des fractions décimales.}$$

La fraction décimale $\frac{1}{10}$ est une unité décimale du premier ordre ou dixième;

La fraction décimale $\frac{1}{100}$ est une unité décimale du second ordre ou centième;

La fraction décimale $\frac{1}{1\,000}$ est une unité décimale du troisième ordre ou millième...

270. Nombre rationnel décimal.

Un nombre rationnel est dit nombre décimal si dans sa classe d'équivalence figure une fraction décimale.

Ainsi le nombre rationnel représenté par la fraction $\frac{1\,669}{200}$ est un nombre décimal car on a :

$$\frac{1\,669}{200} = \frac{8\,345}{1\,000}$$

et la fraction décimale $\frac{8\,345}{1\,000}$ est équivalente à $\frac{1\,669}{200}$.

De plus, si on considère le nombre $\frac{8\,345}{1\,000}$, on peut écrire

$$\frac{8\,345}{1\,000} = 8 + \frac{3}{10} + \frac{4}{100} + \frac{5}{1\,000}.$$

On convient alors d'écrire :

$$\frac{8\,345}{1\,000} = 8{,}345$$

8,345 est *la représentation décimale;* 8 est la *partie entière;* et les chiffres placés à la droite de la virgule constituent la *partie décimale du nombre.*

Donc :

Pour obtenir le nombre décimal égal à une fraction décimale donnée on sépare par une virgule, à la droite du numérateur, autant de chiffres décimaux qu'il y a de zéros au dénominateur.

Inversement :

La fraction décimale égale à un nombre décimal donné est une fraction dont le numérateur est le nombre entier obtenu en supprimant la virgule et dont le dénominateur est l'unité suivie d'autant de zéros qu'il y a de chiffres décimaux après la virgule dans le nombre donné.

271. Condition pour qu'un rationnel soit décimal.

Soit le rationnel représenté par la fraction $\frac{a}{b}$, que l'on suppose irréductible. On se propose de chercher à quelle condition il existe une fraction décimale $\frac{A}{10^n}$ tel que $\frac{a}{b} = \frac{A}{10^n}$, c'est-à-dire telle que

$$\frac{a}{b} = \frac{A}{2^n \cdot 5^n}.$$

Une condition nécessaire et suffisante pour que la fraction irréductible $\frac{a}{b}$ soit équivalente à $\frac{A}{10^n}$ est donc que b divise $2^n \cdot 5^n$; d'où :

Une condition nécessaire et suffisante pour qu'une fraction irréductible soit équivalente à une fraction décimale est que son dénominateur n'admette pas dans sa décomposition d'autres facteurs premiers que 2 et 5.

CHAPITRE XXIV

LE CORPS R DES RÉELS

272. Sections minorées de Q.

Soit α une partie de Q : $\alpha \subset Q$ ou $\alpha \in \mathcal{P}(Q)$.
On dit que cette partie α de Q est une section minorée de Q, ou une section finissante si elle possède les propriétés suivantes :

[S1] $\alpha \neq \varnothing$ **et** $\alpha \neq Q$.

[S2] $(\forall a)(\forall b)$ $(a \in \alpha$ **et** $a \leqslant b) \Rightarrow (b \in \alpha)$.

On définit de même une *section majorée* ou *section commençante de Q*.

273. Sections ouvertes. Sections fermées.

Si une section minorée α possède un plus petit élément elle est dite fermée; si elle ne possède pas de plus petit élément elle est dite ouverte.

Une section minorée ouverte est donc caractérisée par les trois propriétés :

[S1] $\alpha \neq \varnothing$ **et** $\alpha \neq Q$.

[S2] $(\forall a)(\forall b)$ $(a \in \alpha$ **et** $a \leqslant b) \Rightarrow (b \in \alpha)$.

[S3] ***α n'a pas de plus petit élément.***

274. Exemples.

◇ *Exemple 1.*

Soit la partie α de Q définie par

$$\alpha = \{ x/x \in Q \quad \text{et} \quad 2 \leqslant x \}$$

α est une section minorée; en effet elle vérifie les deux propriétés précédentes.

S1 α n'est pas vide : 3, par exemple, appartient à α

α n'est pas identique à Q : 0, par exemple n'appartient pas à α.

S2 Si a appartient à α et si $a \leqslant b$, on a $2 \leqslant a \leqslant b$, donc b appartient à α.

De plus, 2 est plus petit élément de α, donc α est une section finissante fermée.

◇ *Exemple 2.*

Soit la partie α de Q définie par

$$\alpha = \{ x/x \in Q \quad \text{et} \quad -2 < x \}$$

On démontre, comme pour l'exemple 1, que α est une section finissante.

Mais ici, il n'y a pas de plus petit élément : $-2 \in \complement_Q(\alpha)$. Donc α est une section finissante ouverte.

◇ *Exemple 3.*

Soit la partie α de Q.

$$\alpha = \{ x/x \in Q \quad \text{et} \quad 2 < x^2 \}$$

C'est une section minorée; en effet elle vérifie les trois propriétés :

S1 $\alpha \neq \varnothing$, car 4 appartient à α;

$\alpha \neq$ Q, car 0 n'appartient pas à α.

S2 Si $a \in \alpha$ et $a \leqslant b$, on a $2 < a^2 \leqslant b^2$ (car a étant positif, b est aussi positif), et par suite b appartient à α.

S3 α n'a pas de plus petit élément, car il n'y a aucun rationne dont le carré est 2.

α est donc une section minorée ouverte.

◇ *Exemple 4.*

Soit la partie α de Q définie par

$$\alpha = \{ x/x \in Q \quad \text{et} \quad 2 < x < 3 \}$$

α n'est pas une section minorée car si on considère $a = \frac{5}{2}$ et $b = 4$, on a $a \in \alpha$ et $a \leqslant b$ et cependant b n'appartient pas à α : la propriété S2 n'est pas vérifiée. On notera cependant que les propriétés S1 et S3 sont vérifiées.

275. Nombres réels.

On appelle nombre réel toute section minorée ouverte de Q. L'ensemble des nombres réels est noté R.

276. Complémentaire d'une section minorée.

Soit une section minorée α de Q. On peut envisager $\alpha_1 = \complement_Q(\alpha)$. α_1 est une section majorée.

◇ *Exemple 1.*

Soit :

$$\alpha = \{ x/x \in Q \quad \text{et} \quad 2 \leqslant x \}$$

qui est une section minorée fermée. On a :

$$\alpha_1 = \complement_Q \alpha = \{ x/x \in Q \quad \text{et} \quad x < 2 \}$$

α_1 est donc une section majorée ouverte.

◇ *Exemple 2.*

Soit :

$$\alpha = \{ x/x \in Q \quad \text{et} \quad -2 < x \}$$

qui est une section minorée ouverte. On a :

$$\alpha_1 = \complement_Q \alpha = \{ x/x \in Q \quad \text{et} \quad x \leqslant -2 \}$$

α_1 est donc une section majorée fermée.

◇ *Exemple 3.*

Soit :

$$\alpha = \{ x/x \in Q \quad \text{et} \quad 2 < x^2 \}$$

qui est une section minorée ouverte. On a :

$$\alpha_1 = \complement_Q \alpha = \{ x/x \in Q \quad \text{et} \quad x^2 < 2 \}$$

α_1 est donc une section majorée ouverte. On voit que dans ce cas α et α_1 sont des sections ouvertes.

277. Plongement de Q dans R.

A tout nombre rationnel a on fait correspondre le nombre réel α défini par

$$\alpha = \{ x/x \in Q \quad \text{et} \quad a < x \}$$

Donc :

φ : $$a \in Q \longrightarrow \varphi(a) = \alpha \in R,$$

Cette application φ est injective, car

$$a \neq b \Rightarrow \varphi(a) \neq \varphi(b),$$

mais elle n'est pas surjective, car, par exemple, le réel

$$\alpha = \{ x/x \in Q \quad \text{et} \quad 2 < x^2 \}$$

n'est pas l'image d'un rationnel.

Soit R′ l'ensemble des réels de la forme $\varphi(a)$, φ est alors une bijection de Q sur R′. Cela autorise à poser

$$\varphi(a) = a = \alpha$$

c'est-à-dire à identifier Q et R′ : on a alors *plongé, ou immergé, Q dans R.*

On a donc :

$$\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R}.$$

Les nombres appartenant à $\complement_R Q$ sont appelés les nombres irrationnels.

278. Addition des nombres réels.

1° Soient deux nombres réels α et β. On considère l'ensemble :

$$\sigma = \{ x = x_1 + x_2/x_1 \in \alpha \quad \text{et} \quad x_2 \in \beta \}$$

L'ensemble σ est une section minorée; en effet, elle vérifie les trois propriétés :

$\boxed{S_1}$ $\sigma \neq \varnothing$, car α et β étant des sections minorées, il existe $a \in \alpha$ et $b \in \beta$, donc $a + b \in \sigma$.

$\sigma \neq Q$, car α et β étant des sections minorées, il existe $a' \notin \alpha$ et $b' \notin \beta$ donc $a' + b' \notin \sigma$.

$\boxed{S_2}$ Soient $a \in \sigma$ et $b \in Q$ avec $a \leqslant b$. Puisque a appartient à σ, il existe $a_1 \in \alpha$ et $a_2 \in \beta$ tel que $a = a_1 + a_2$.

Or :

$$\begin{aligned} b &= a + (b - a) \\ &= a_1 + (a_2 + b - a) \end{aligned}$$

$b - a$ étant positif ou nul, $a_2 \leqslant a_2 + b - a$, donc $a_2 + b - a$ appartient à β.

b est alors la somme de $a_1 \in \alpha$ et de $a_2 + b - a \in \beta$; ce qui prouve que $b \in \sigma$.

$\boxed{S_3}$ α et β n'ayant pas de plus petit élément, l'ensemble des sommes $x = x_1 + x_2$ n'a pas de plus petit élément.

Ainsi σ est une section minorée ouverte.

2° σ étant une section minorée ouverte, c'est-à-dire un nombre réel, on peut donner la définition suivante :

Si** α **et** β **sont deux nombres réels, le nombre

$$\sigma = \{ x = x_1 + x_2 / x_1 \in \alpha \quad \text{et} \quad x_2 \in \beta \}$$

***est la somme de** α **et** β.*

On pose :

$$\sigma = \alpha + \beta.$$

279. Commutativité de l'addition des réels.

Soient deux nombres réels α et β. On a :

$$\alpha + \beta = \{ x = x_1 + x_2 / x_1 \in \alpha \quad \text{et} \quad x_2 \in \beta \}$$

et

$$\beta + \alpha = \{ x = x_2 + x_1 / x_1 \in \alpha \quad \text{et} \quad x_2 \in \beta \}$$

Or : $x_1 + x_2 = x_2 + x_1$. Donc :

C $\qquad (\forall \alpha)\ (\forall \beta) \qquad \alpha + \beta = \beta + \alpha.$

Et :

L'addition des nombres réels est commutative.

280. Associativité de l'addition des réels.

Soient trois nombres réels α, β, γ. On a :

$$(\alpha + \beta) + \gamma = \{ x = (x_1 + x_2) + x_3 / x_1 \in \alpha,\ x_2 \in \beta;\ x_3 \in \gamma \}$$

et

$$\alpha + (\beta + \gamma) = \{ x = x_1 + (x_2 + x_3) / x_1 \in \alpha,\ x_2 \in \beta;\ x_3 \in \gamma \}$$

Or : $(x_1 + x_2) + x_3 = x_1 + (x_2 + x_3)$. Donc :

A $\qquad (\forall \alpha)\ (\forall \beta)\ (\forall \gamma) \qquad (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma).$

Et :

L'addition des nombres réels est associative.

281. Elément neutre pour l'addition.

On considère le nombre réel associé au nombre rationnel 0 dans le plongement de Q dans R, c'est-à-dire :

$$0 = \varphi(0) = \{ x / x \in Q \quad \text{et} \quad 0 < x \}$$

On se propose de montrer que $\varphi(0) = 0$ est neutre pour l'addition.
Soit α un nombre réel quelconque.

$\alpha + 0 \subset \alpha$.

Si $x \in \alpha + 0$, on a $x = x_1 + x_2$ avec $x_1 \in \alpha$ et $x_2 \in 0$.
x_2 est positif et par suite $x = x_1 + x_2$ est supérieur à $x_1 : x > x_1$. Comme x_1 appartient à α, $x > x_1$ appartient aussi à α.

Donc :

$$\alpha + 0 \subset \alpha.$$

$\alpha \subset \alpha + 0$.

Soit un élément x de α.
Puisque α n'a pas de plus petit élément, il existe un rationnel x_1 appartenant à α et inférieur à x. D'où :

$$x = x_1 + (x - x_1)$$

avec $x_1 \in \alpha$, et $x - x_1 > 0$ ou $x - x_1 \in 0$. Cela signifie que x appartient à $\alpha + 0$.

Donc :

$$\alpha \subset \alpha + 0.$$

L'antisymétrie de l'inclusion montre alors que $\alpha + 0 = \alpha$.

En tenant compte de la commutativité de l'addition, on a :

N $\qquad (\forall \alpha) \qquad \alpha + 0 = 0 + \alpha = \alpha$

Et :

$0 = \varphi(0)$ est neutre pour l'addition des réels.

282. R est symétrisé pour l'addition.

Soit un nombre réel quelconque α.
On considère l'ensemble

$$a_1 = \{ -x / x \in \alpha \}$$

C'est une section majorée ouverte.
$\complement_Q(\alpha_1)$ est une section minorée.
Si elle est ouverte, on pose $\alpha' = \complement_Q \alpha_1$.
Si elle est fermée, elle a un plus petit élément; on enlève ce plus petit élément, et on désigne par α' la section minorée ouverte ainsi obtenue.

On se propose de montrer que α' est le symétrique de α pour l'addition.

$\alpha + \alpha' \subset 0$.

Si $x \in \alpha + \alpha'$, on a : $x = x_1 + x_2$ avec : $x_1 \in \alpha$ et $x_2 \in \alpha'$.

x_2 appartenant à α', $-x_2$ appartient à $\complement_Q \alpha'$, c'est-à-dire que $-x_2$ n'appartient pas à α; par suite :

$$-x_2 < x_1$$

ou (propriété de l'ordre dans Q)

$$x_1 + x_2 > 0$$

et $$x = x_1 + x_2 \in 0.$$

Donc :

$$\alpha + \alpha' \subset 0.$$

$0 \subset \alpha + \alpha'$.

Soit $x \in 0$, c'est-à-dire $x > 0$.

En prenant x_1, dans α, suffisamment petit(1), $-x_1 \in \complement_Q \alpha$; et $-x_1$ est suffisamment grand pour que $-x_1 + x$ appartienne à α'. On pose alors :

$$-x_1 + x = x_2$$

et :

$$x = x_1 + x_2$$

avec : $x_1 \in \alpha$ et $x_2 \in \alpha'$.

L'égalité $x = x_1 + x_2$ prouve alors que $x \in \alpha + \alpha'$ et :

$$0 \subset \alpha + \alpha'.$$

L'antisymétrie de l'inclusion montre alors que $\alpha + \alpha' = 0$.

En tenant compte de la commutativité de l'addition, on a :

[S] $$(\forall \alpha)\ (\exists \alpha') : \quad \alpha + \alpha' = \alpha' + \alpha = 0.$$

Et :

Tous les nombres réels sont symétrisables pour l'addition.

On pose : $\alpha' = -\alpha$; et $-\alpha$ est l'opposé de α.

Tous les nombres réels sont réguliers pour l'addition.

283. Groupe additif.

L'addition des nombres réels possède les propriétés [A] [N] [S] [C].

Donc :

L'ensemble R, muni de l'addition, est un groupe additif commutatif.

---

(1) Raisonnement partiellement intuitif.

284. Régularité.

Soient trois réels α, β et μ.

On suppose que l'on a :

$$\alpha + \mu = \beta + \mu$$

En ajoutant $-\mu$ aux deux membres de cette égalité, on obtient :

$$(\alpha + \mu) + (-\mu) = (\beta + \mu) + (-\mu)$$

ou

$$\alpha + [\mu + (-\mu)] = \beta + [\mu + (-\mu)]$$

ou

$$\alpha + 0 = \beta + 0$$

ou

$$\alpha = \beta$$

Donc :

$$(\forall\alpha)\ (\forall\beta)\ (\forall\mu) : \quad \alpha + \mu = \beta + \mu \Rightarrow \alpha = \beta.$$

Et :

Tous les nombres réels sont réguliers pour l'addition.

285. Soustraction.

Soient $\alpha \in R$ ***et*** $\beta \in R$.

Trouver un réel x ***tel que***

$$\alpha = \beta + x$$

s'appelle soustraire β ***de*** α.

En ajoutant $-\beta$ aux deux membres de l'égalité précédente, on obtient :

$$\begin{aligned}(-\beta) + \alpha &= (-\beta) + \beta + x \\ &= 0 + x \\ &= x\end{aligned}$$

Le réel cherché est donc :

$$x = \alpha + (-\beta)$$

Et :

Pour soustraire un réel on ajoute son opposé.

Le nombre x est la différence entre α et β. On le note :

$$x = \alpha - \beta$$

D'où :

$$\alpha - \beta = \alpha + (-\beta)$$

286. Conséquences.

1° Soit :

$$x = \alpha - (\beta + \gamma)$$

α, β, γ étant des réels; on a :

$$[x = \alpha - (\beta + \gamma)] \Leftrightarrow [x + \beta + \gamma = \alpha] \Leftrightarrow [x + \gamma = \alpha - \beta] \Leftrightarrow [x = \alpha - \beta - \gamma]$$

D'où la formule :

$$\alpha - (\beta + \gamma) = \alpha - \beta - \gamma.$$

2° En particulier :

$$-(\beta + \gamma) = -\beta - \gamma.$$

3° Soit :

$$x = \alpha - (\beta - \gamma)$$

α, β, γ étant des réels; on a :

$$[x = \alpha - (\beta - \gamma)[\Leftrightarrow [x + \beta - \gamma = \alpha] \Leftrightarrow [x + \beta = \alpha + \gamma] \Leftrightarrow [x = \alpha - \beta + \gamma]$$

D'où la formule :

$$\alpha - (\beta - \gamma) = \alpha - \beta + \gamma.$$

4° En particulier :

$$-(\beta - \gamma) = -\beta + \gamma.$$

287. Réels positifs. Réels négatifs.

1° Soit un nombre réel α quelconque :

Si, quel que soit $x \in \alpha$, x est positif, le nombre α est dit positif.
Si il existe dans α un élément x négatif, le nombre α est dit négatif.

2° *L'ensemble des nombres réels positifs se note R_+.* R_+ contient 0.

On pose :

$$R^* = R - \{ 0 \}$$

et

$$R_+^* = R_+ - \{ 0 \}.$$

Les éléments de R_+^* sont les réels strictement positifs.
On représente par R_- l'ensemble des réels strictement négatifs.

3° Un nombre réel α et son opposé $-\alpha$ sont évidemment de signes opposés, c'est-à-dire que l'un est positif et l'autre négatif.

288. Comparaison des réels.

1° ***Le nombre réel α est dit inférieur à β si $\alpha - \beta$ est négatif.***
On écrit :

$$\alpha < \beta$$

Et :

$$(\alpha < \beta) \Leftrightarrow (\alpha - \beta \in R_-)$$

2° ***Le nombre réel α est dit strictement supérieur à β si $\alpha - \beta$ est strictement positif.***

On écrit :

$$\alpha > \beta$$

Et :

$$(\alpha > \beta) \quad \Leftrightarrow \quad (\alpha - \beta \in R_+^*).$$

3° ***Si $\alpha \in R_-$, α est inférieur à 0.***

En effet :

$$(\alpha \in R_-) \quad \Leftrightarrow \quad (\alpha - 0 \in R_-) \quad \Leftrightarrow \quad (\alpha < 0).$$

De même :

$$(\alpha \in R_+^*) \quad \Leftrightarrow \quad (\alpha > 0).$$

289. Valeur absolue d'un réel.

1° Soit $\alpha \in R$. On définit une application de R dans R_+ par

$$v : \quad \alpha \longrightarrow v(\alpha) = \alpha \quad \text{si} \quad \alpha \geqslant 0$$
$$\alpha \longrightarrow v(\alpha) = -\alpha \quad \text{si} \quad \alpha < 0$$

$v(\alpha)$ est la valeur absolue de α; on note $v(\alpha) = |\alpha|$

Donc :

$$|\alpha| = \alpha, \quad \textit{si} \quad \alpha \geqslant 0$$
$$|\alpha| = -\alpha, \quad \textit{si} \quad \alpha < 0.$$

2° On a immédiatement :

$$|-\alpha| = |\alpha|$$

et

$$|\alpha| = 0 \Leftrightarrow \alpha = 0.$$

3° Si $\alpha > 0$, on peut écrire : $\alpha = |\alpha|$

Si $\alpha < 0$, on peut écrire : $\alpha = -|\alpha|$

290. Les règles de l'addition.

1° **Les deux nombres réels α et β sont de même signe.**

Si α et β sont positifs, on a :

$$\alpha + \beta = |\alpha| + |\beta|$$
et $|\alpha + \beta| = |\alpha| + |\beta|$

Si α *et* β *sont négatifs*, on a :

$$\alpha + \beta = -|\alpha| - |\beta|$$

ou

$$\alpha + \beta = -(|\alpha| + |\beta|)$$

$$\text{et} \quad |\alpha + \beta| = |\alpha| + |\beta|$$

Donc :

La somme de deux nombres réels de même signe est un nombre réel
— dont le signe est le signe commun
— dont la valeur absolue est la somme des valeurs absolues des deux nombres.

2° Les deux nombres réels α et β sont de signes opposés.

On peut supposer : $\alpha > 0$ et $\beta < 0 : \alpha = |\alpha|$ et $\beta = -|\beta|$

D'où :

$$\alpha + \beta = |\alpha| - |\beta|$$

Si $|\alpha| > |\beta|$, on a :

$$\alpha + \beta = |\alpha| - |\beta|$$

$\alpha + \beta$ est positif; et $$|\alpha + \beta| = |\alpha| - |\beta|$$

Si $|\alpha| < |\beta|$, on a :

$$\alpha + \beta = |\alpha| - |\beta|$$

$\alpha + \beta$ est négatif et $$|\alpha + \beta| = |\beta| - |\alpha| = \big||\alpha| - |\beta|\big|$$

La somme de deux nombres réels de signes opposés est un nombre réel
— dont le signe est le signe du nombre qui a la plus grande valeur absolue;
— dont la valeur absolue est la différence des valeurs absolues des deux nombres.

291. Valeurs absolues d'une somme et d'une différence.

Comme dans Q (cf. n° 259) on a les inégalités suivantes :

$$\big||\alpha| - |\beta|\big| \leqslant |\alpha + \beta| \leqslant |\alpha| + |\beta|$$

et

$$\big||\alpha| - |\beta|\big| \leqslant |\alpha - \beta| \leqslant |\alpha| + |\beta|.$$

292. Multiplication des réels positifs.

Soient deux nombres réels positifs α et β. On considère l'ensemble

$$\pi = \{ x = x_1 x_2 / x_1 \in \alpha \quad \text{et} \quad x_2 \in \beta \}$$

L'ensemble π est une section minorée; en effet, elle vérifie les trois propriétés :

$\boxed{S_1}$ $\pi \neq \varnothing$, car α et β étant des sections minorées, il existe $a \in \alpha$ et $b \in \beta$, donc $ab \in \pi$.

$\pi \neq Q$, car α et β étant des sections minorées, il existe $a' \notin \alpha$ ($a' \in R_+$) et $b' \notin \beta$ ($b' \in R_+$), donc $a'b' \notin \pi$.

$\boxed{S_2}$ Soient $a \in \pi$ et $b \in Q$ avec $a \leqslant b$. Puisque a appartient à π, il existe $a_1 \in \alpha$ et $a_2 \in \beta$ tels que $a = a_1 a_2$.

Or :

$$b = a \cdot \frac{b}{a}$$
$$= a_1 \cdot \left(a_2 \cdot \frac{b}{a}\right)$$

$\frac{b}{a}$ étant supérieur ou égal à 1, on a $a_2 \leqslant a_2 \cdot \frac{b}{a}$, donc $a_2 \cdot \frac{b}{a}$ appartient à β. b est alors le produit de $a_1 \in \alpha$ et de $a_2 \cdot \frac{b}{a} \in \beta$; ce qui prouve que b appartient à π.

$\boxed{S_3}$ α et β n'ayant pas de plus petit élément, l'ensemble des produits $x = x_1 x_2$ n'a pas de plus petit élément.

Ainsi π est une section minorée ouverte.

2° π étant une section minorée ouverte, c'est-à-dire un nombre réel, on peut donner la définition suivante :

Si α et β sont deux nombres réels positifs, le nombre réel positif

$$\pi = \{ x = x_1 x_2 / x_1 \in \alpha \quad \text{et} \quad x_2 \in \beta \}$$

est le produit de α et β.

On pose :

$$\pi = \alpha \cdot \beta$$

293. Commutativité de la multiplication des réels positifs.

Soient deux nombres réels positifs α et β. On a :

$$\alpha\beta = \{ x = x_1 x_2 / x_1 \in \alpha \ \text{ et } \ x_2 \in \beta \}$$

et

$$\beta\alpha = \{ x = x_2 x_1 / x_1 \in \alpha \ \text{ et } \ x_2 \in \beta \}.$$

Or : $x_1x_2 = x_2x_1$. Donc :

C $$(\forall\alpha)\ (\forall\beta)\quad \alpha\beta = \beta\alpha.$$

Et :

La multiplication des réels positifs est commutative.

294. Associativité de la multiplication des réels positifs.

Soient trois nombres réels positifs α, β, γ. On a :

$$(\alpha\beta)\gamma = \{ x = (x_1x_2)\ x_3/x_1 \in \alpha;\ x_2 \in \beta;\ x_3 \in \gamma \}$$

et

$$\alpha(\beta\gamma) = \{ x = x_1(x_2x_3)/x_1 \in \alpha;\ x_2 \in \beta;\ x_3 \in \gamma \}$$

Or : $(x_1x_2)x_3 = x_1(x_2x_3)$. Donc :

A $$(\forall\alpha)\ (\forall\beta)\ (\forall\gamma)\ :\quad (\alpha\beta)\gamma = \alpha(\beta\gamma).$$

Et :

La multiplication des réels positifs est associative.

295. Elément neutre pour la multiplication des réels positifs.

On considère le nombre réel positif associé au nombre rationnel 1 dans le plongement de Q dans R, c'est-à-dire :

$$1 = \varphi(1) = \{ x/x \in Q \quad \text{et} \quad 1 < x \}$$

On se propose de montrer que $\varphi(1) = 1$ est neutre pour la multiplication dans R_+.

Soit α un nombre réel positif quelconque.

$\alpha \times 1 \subset \alpha$.

Si $x \in \alpha \times 1$, on a : $x = x_1x_2$ avec $x_1 \in \alpha$ et $x_2 \in 1$.

x_2 est supérieur à 1, donc x est supérieur à x_1. Comme x_1 appartient à α, il en est de même de x.

Ainsi :

$$\alpha \times 1 \subset \alpha.$$

$\alpha \subset \alpha \times 1$.

Soit un élément x de α.

Puisque α n'a pas de plus petit élément(1), il existe un rationnel x_1 appartenant à α et inférieur à x : $x_1 < x$ ou $1 < \frac{x}{x_1}$.

(1) Raisonnement partiellement intuitif.

D'où :

$$x = x_1 \times \frac{x}{x_1}$$

avec $x_1 \in \alpha$ et $\frac{x}{x_1} \in 1$; cela signifie que x appartient à $\alpha \times 1$.

Donc :

$$\alpha \subset \alpha \times 1.$$

L'antisymétrie de l'inclusion montre que $\alpha \times 1 = \alpha$.

En tenant compte de la commutativité de la multiplication, on a :

N $$(\forall \alpha) : \quad \alpha \times 1 = 1 \times \alpha = \alpha.$$

Et :

1 = φ(1) est neutre pour la multiplication des réels positifs.

296. Inverse d'un réel positif.

Soit un nombre réel positif non nul α :

$$\alpha \in R_+ - \{0\}$$

On considère l'ensemble :

$$\alpha_1 = \left\{ \frac{1}{x} \middle/ x \in \alpha \right\} \cup (R_-).$$

C'est une section majorée ouverte.

$\complement_Q(\alpha_1)$ est une section minorée.

Si elle est ouverte on pose : $\alpha' = \complement_Q \alpha_1$.

Si elle est fermée, elle a un plus petit élément; on enlève ce plus petit élément, et on désigne par α' la section minorée ainsi obtenue.

On se propose de montrer que α' est le symétrique de α pour la multiplication,

$\alpha \cdot \alpha' \subset 1.$

Si $x \in \alpha\alpha'$, on a : $x = x_1 x_2$ avec $x_1 \in \alpha$ et $x_2 \in \alpha'$.

x_2 appartenant à α', $\frac{1}{x_2}$ appartient à $\complement_{Q+}\alpha'$, c'est-à-dire que $\frac{1}{x_2}$ n'appartient pas à α; par suite :

$$\frac{1}{x_2} < x_1$$

ou

$$1 < x_1 x_2$$

et $x = x_1 x_2$ appartient à 1.

Donc :

$$\alpha\alpha' \subset 1.$$

$1 \subset \alpha \cdot \alpha'$.

Soit $x \in 1$, c'est-à-dire : $1 < x$.

En prenant x_1, dans α, suffisamment petit, $\frac{1}{x_1} \in \complement_{Q_+}(\alpha)$ et $\frac{1}{x_1}$ est suffisamment grand pour que $\frac{x}{x_1}$ appartiennent à α'.

On pose :

$$\frac{x}{x_1} = x_2$$

et

$$x = x_1 x_2$$

avec : $x_1 \in \alpha$ et $x_2 \in \alpha'$. Cela prouve que $x \in \alpha\alpha'$. Et :

$$1 \subset \alpha\alpha'.$$

L'antisymétrie de l'inclusion montre alors que $\alpha\alpha' = 1$.

En tenant compte de la commutativité de la multiplication dans R_+, on a :

[S] $$(\forall\alpha)\ (\alpha \in R_+^*)\ (\exists\alpha') : \quad \alpha\alpha' = \alpha'\alpha = 1.$$

Et :

Tous les nombres réels de R_+^* sont symétrisables pour la multiplication.

On pose : $\alpha' = \alpha^{-1} = \frac{1}{\alpha}$, et on dit que α' est l'inverse de α.

297. Distributivité dans R_+.

Soient des nombres réels positifs α, β et μ. On a :

$$\mu(\alpha + \beta) = \{\ x = m(x_1 + x_2)/m \in \mu;\ x_1 \in \alpha;\quad x_2 \in \beta\ \}$$

et

$$\mu\alpha + \mu\beta = \{\ x = mx_1 + mx_2/m \in \mu;\ x_1 \in \alpha;\quad x_2 \in \beta\ \}$$

Or : $m(x_1 + x_2) = mx_1 + mx_2$. Donc :

$$(\forall\alpha)\ (\forall\beta)\ (\forall\mu) : \quad \mu(\alpha + \beta) = \mu\alpha + \mu\beta.$$

Et :

La multiplication des réels positifs est distributive pour l'addition des réels positifs.

298. Prolongement de la multiplication de R_+ à R.

On peut prolonger la multiplication définie dans R_+ à R de la façon suivante :

Le produit de deux réels de même signe est un réel positif; le produit de deux réels de signes opposés est un réel négatif; dans les deux cas la valeur absolue du produit est le produit des valeurs absolues.

Si l'un des deux nombres est nul, le produit est nul.

Cette extension de la multiplication est compatible avec la multiplication dans $Q \subset R$, puisque les règles énoncées plus haut sont identiques à celles de la multiplication dans Q.

On a, si $\alpha \in R$ et $\alpha' \in R$:

$$|\alpha\alpha'| = |\alpha| \cdot |\alpha'|.$$

299. Propriétés de la multiplication des réels.

La multiplication des réels possède les propriétés suivantes :

Commutativité :

Soient deux réels quelconques α et β.

Les produits $\alpha\beta$ et $\beta\alpha$ ont le même signe, et $|\beta\alpha| = |\alpha\beta| = |\alpha|.|\beta|$; donc :

[C] $$(\forall\alpha)\ (\forall\beta) : \quad \alpha\beta = \beta\alpha.$$

Et :

La multiplication des réels est commutative.

Associativité.

Soient trois réels quelconques α, β, γ.

Les produits $(\alpha\beta)\gamma$ et $\alpha(\beta\gamma)$ ont le même signe et $|(\alpha\beta)\cdot\gamma| = |\alpha\cdot(\beta\gamma)| = |\alpha|\cdot|\beta|\cdot|\gamma|$.

Donc :

[A] $$(\forall\alpha)\ (\forall\beta)\ (\forall\gamma) : \quad (\alpha\beta)\gamma = \alpha(\beta\gamma).$$

Et :

La multiplication des réels est associative.

Elément neutre pour la multiplication.

Soient les réels α et 1.

$\alpha\cdot 1$ et α ont le même signe et $|\alpha \times 1| = |\alpha| \times |1| = |\alpha|$.

Donc :

[N] $(\forall \alpha) \quad \alpha \times 1 = 1 \times \alpha = \alpha.$

Et :

Le nombre réel 1 est neutre pour la multiplication des réels.

R* est symétrisé pour la multiplication.

Soit un nombre réel quelconque non nul : $\alpha \in R^*$.

On considère le nombre α', de même signe que α, et dont la valeur absolue $|\alpha'|$ est l'inverse du nombre réel positif $|\alpha|$:

$$|\alpha'| = \frac{1}{|\alpha|}.$$

Par suite, le produit $\alpha\alpha'$ est positif et $|\alpha\alpha'| = |\alpha| \cdot |\alpha'| = 1$. Autrement dit :

[S] $(\forall \alpha)\ (\exists \alpha') : \quad \alpha\alpha' = \alpha'\alpha = 1.$

Et :

Tous les réels, non nuls, sont symétrisés pour la multiplication.

α' est l'inverse de α; $\quad \alpha' = \alpha^{-1} = \dfrac{1}{\alpha}.$

300. Groupe multiplicatif.

L'ensemble $R^* = R - \{0\}$ est muni d'une multiplication possédant les propriétés [A][N][S][C].

Donc :

Les nombres réels, non nuls, forment un groupe multiplicatif commutatif.

301. Régularité.

Soient les trois nombres réels α, β, μ $(\alpha \in R;\ \beta \in R;\ \mu \in R^*)$.

On suppose que l'on a :

$$\alpha\mu = \beta\mu$$

En multipliant par μ^{-1} les deux membres de cette égalité, on obtient :

$$(\alpha\mu) \cdot \mu^{-1} = (\beta\mu)\mu^{-1}$$

ou

$$\alpha(\mu \cdot \mu^{-1}) = \beta \cdot (\mu \cdot \mu^{-1})$$

ou

$$\alpha \times 1 = \beta \cdot 1$$

ou

$$\alpha = \beta.$$

Donc :

$(\forall\alpha)\ (\alpha \in R)\ (\forall\beta)\ (\beta \in R)\ (\forall\mu)\ (\mu \in R^*)\ :\ \alpha\mu = \beta\mu \Rightarrow \alpha = \beta.$

Et :

Tous les réels, non nuls, sont réguliers pour la multiplication.

302. Division.

Soient $\alpha \in R$ ***et*** $\beta \in R^*$.

Trouver un nombre réel x, (x∈R), tel que

$$\alpha = \beta \mathbf{x}$$

s'appelle diviser α ***par*** β.

En multipliant les deux membres de l'égalité précédente par β^{-1}, on obtient :

$$\begin{aligned}\beta^{-1} \cdot \alpha &= \beta^{-1} \cdot (\beta x)\\ &= (\beta^{-1} \cdot \beta) x\\ &= 1 \times x\\ &= x.\end{aligned}$$

Le nombre x cherché est donc :

$$x = \alpha \times \beta^{-1} = \alpha \times \frac{1}{\beta}.$$

Et :

Pour diviser par un nombre réel, on multiplie par son inverse.

On note :

$$x = \frac{\alpha}{\beta}$$

et

$$\frac{\alpha}{\beta} = \alpha \times \frac{1}{\beta}.$$

303. Distributivité de la multiplication pour l'addition.

Les règles de l'addition (cf. nº 290) et de la multiplication (cf. nº 298) permettent d'étendre la distributivité démontrée par R_+ à R.

Donc :

$\boxed{D}$ $(\forall\alpha)\ (\forall\beta)\ (\forall\mu) :\quad \mu(\alpha+\beta) = \mu\alpha + \mu\beta$

$$(\alpha+\beta)\mu = \alpha\mu + \beta\mu.$$

Et :

La multiplication des réels est distributive pour l'addition des réels.

304. Le corps R des réels.

L'ensemble R des réels est muni d'une loi de composition interne, notée additivement, et douant R d'une structure de groupe commutatif, c'est-à-dire possédant les propriétés $\boxed{A}\boxed{N}\boxed{S}\boxed{C}$.

L'ensemble R est muni d'une seconde loi de composition interne, notée multiplicativement, et douant R* d'une structure de groupe commutatif, c'est-à-dire possédant les propriétés $\boxed{A}\boxed{N}\boxed{S}\boxed{C}$.

De plus la multiplication est distributive pour l'addition.

Ainsi :

R est le corps commutatif des réels.

305. Remarque.

Au n° 277, on a immergé Q dans R.
Les règles de l'addition et de la multiplication dans R sont identiques aux règles de l'addition et de la multiplication dans Q.

Donc :

L'application φ respecte l'addition et la multiplication.

306. Relation d'ordre total.

La relation d'inégalité-égalité, notée $\leqslant$, est une relation d'ordre total.

En effet cette relation possède les propriétés suivantes :

Réflexivité :

$$\alpha \leqslant \alpha$$

car

$$\alpha - \alpha = 0.$$

Antisymétrie :

$$(\alpha \leqslant \beta \quad \text{et} \quad \beta \leqslant \alpha) \Rightarrow \alpha = \beta$$

car

$$(\alpha - \beta \leqslant 0 \quad \text{et} \quad \beta - \alpha \leqslant 0) \Rightarrow (\alpha - \beta = 0) \Rightarrow \alpha = \beta.$$

Transitivité :

$$(\alpha \leqslant \beta \quad \text{et} \quad \beta \leqslant \gamma) \Rightarrow \alpha \leqslant \gamma$$

car de

$$\alpha - \beta \leqslant 0 \quad \text{et} \quad \beta - \gamma \leqslant 0$$

on tire :

$$\alpha - \beta + \beta - \gamma \leqslant 0$$

ou

$$\alpha - \gamma \leqslant 0$$

ou

$$\alpha \leqslant \gamma.$$

De plus l'ordre est total, car deux nombres réels quelconques α et β *sont comparables puisqu'on a* $\alpha \leqslant \beta$ *ou* $\beta \leqslant \alpha$.

307. Addition et ordre.

Soient deux réels α et β tels que

$$\alpha \leqslant \beta.$$

On a :

$$\alpha - \beta \leqslant 0$$

ou

$$\alpha + \gamma - \beta - \gamma \leqslant 0$$

ou

$$\alpha + \gamma \leqslant \beta + \gamma.$$

Donc :

$$(\alpha \leqslant \beta) \Rightarrow (\alpha + \gamma \leqslant \beta + \gamma).$$

Et :

L'addition dans R est compatible avec l'ordre total dans R.

308. Multiplication et ordre.

1° *Soit* μ *un réel positif* $\mu \in R_+^*$.

Si $\alpha > \beta$ ou $\alpha - \beta > 0$, on a :

$$\mu(\alpha - \beta) > 0 \quad \text{ou} \quad \mu\alpha - \mu\beta > 0 \quad \text{ou} \quad \mu\alpha > \mu\beta.$$

Donc :

$$(\mu > 0; \alpha > \beta) \Rightarrow (\mu\alpha > \mu\beta).$$

Si $\alpha < \beta$ ou $\alpha - \beta < 0$, on a :

$$\mu(\alpha - \beta) < 0 \quad \text{ou} \quad \mu\alpha - \mu\beta < 0 \quad \text{ou} \quad \mu\alpha < \mu\beta.$$

Donc :

$$(\mu > 0; \alpha < \beta) \Rightarrow (\mu\alpha < \mu\beta).$$

D'où l'énoncé :

On peut multiplier les deux membres d'une inégalité de nombres réels par un même nombre réel positif sans changer le sens de cette inégalité.

2° *Soit μ un réel négatif :* $\mu \in R_-$

Si $\alpha > \beta$ ou $\alpha - \beta > 0$, on a :

$$\mu(\alpha - \beta) < 0 \quad \text{ou} \quad \mu\alpha - \mu\beta < 0 \quad \text{ou} \quad \mu\alpha < \mu\beta.$$

Donc :

$$(\mu < 0; \alpha > \beta) \Rightarrow (\mu\alpha < \mu\beta).$$

Si $\alpha < \beta$ ou $\alpha - \beta < 0$, on a :

$$\mu(\alpha - \beta) > 0 \quad \text{ou} \quad \mu\alpha - \mu\beta > 0 \quad \text{ou} \quad \mu\alpha > \mu\beta.$$

Donc :

$$(\mu < 0; \alpha < \beta) \Rightarrow (\mu\alpha > \mu\beta).$$

D'où l'énoncé :

On peut multiplier les deux membres d'une inégalité de nombres réels par un même nombre réel négatif à condition de renverser le sens de l'inégalité.

3° *Les deux résultats précédents montre que la multiplication dans R n'est pas compatible avec l'ordre total dans R.*

309. Le corps R est archimédien.

Soient α et β deux réels positifs quelconques avec

$$0 < \alpha < \beta.$$

R est un corps archimédien, car il existe un nombre entier naturel n, (n ∈ N) tel que $n\alpha > \beta$.

En effet, en multipliant cette inégalité par α^{-1}, qui est positif comme α, on obtient $n > \beta \cdot \alpha^{-1}$. Il suffit donc de prendre n supérieur à $\beta\alpha^{-1}$.

310. Le corps R est divisible.

Soient α et β deux réels quelconques avec

$$\alpha < \beta.$$

R est un corps divisible, c'est-à-dire qu'entre les deux réels α et β, il existe au moins un autre réel.

En effet de $\alpha < \beta$ on déduit :

$$\alpha + \beta < 2\beta$$

et

$$2\alpha < \alpha + \beta$$

c'est-à-dire :

$$2\alpha < \alpha + \beta < 2\beta$$

D'où :

$$\alpha < \frac{\alpha + \beta}{2} < \beta.$$

Le nombre $\frac{\alpha + \beta}{2}$ est réel et est compris entre α et β.

311. Conclusion.

L'ensemble R a été muni d'une addition et d'une multiplication qui introduisent dans R une structure de corps commutatif.

Le relation notée $\leqslant$ est une relation d'ordre total.

En conclusion :

L'ensemble R des nombres réels est un corps commutatif, totalement ordonné, archimédien et divisible.

312. Racines d'un nombre réel.

1° Soit un nombre réel positif α. On se propose de chercher, s'il en existe, les nombres a tels que $a^2 = \alpha$.

Un tel nombre a est une racine carrée de α.

2° Le nombre réel positif α définit une section minorée ouverte de R : $\{ x/x \in R, \alpha < x \}$.

On envisage le nombre réel a, positif, défini par la section minorée ouverte de R : $\{ x/x \in R; \alpha < x^2 \}$.

On a bien $a^2 = \alpha$, et d'après la définition même, ce nombre a positif est unique.

Donc :

Un nombre réel positif a une racine carrée réelle positive unique.

On note [1]

$$a = \sqrt{\alpha}.$$

3° Si a est la racine carrée positive de α, le nombre $-a$ est aussi une racine carrée de α, car $(-a)^2 = a^2 = \alpha$. C'est évidemment la seule racine négative.

Donc :

Le nombre réel positif α a deux racines carrées opposées : $\sqrt{\alpha}$ et $-\sqrt{\alpha}$.

4° Un carré étant toujours positif, un nombre réel négatif n'a pas de racine carrée dans le corps R des réels.

Par exemple, il n'existe aucun nombre réel dont le carré est -1. *Une nouvelle extension de la notion de nombre est donc indispensable.*

5° Soit un nombre réel positif α. On se propose de chercher, s'il en existe, les nombres a tels que $a^n = \alpha$. ($n \in \mathrm{N}$).

Un tel nombre a est une racine $\mathbf{n}^{\text{ième}}$ de a.

Comme au 2°, on a :

Un nombre réel positif a une racine $\mathbf{n}^{\text{ième}}$ réelle positive unique.

---

(1) Le symbole $\sqrt{\alpha}$ désigne toujours la racine positive de α : $\sqrt{\alpha} \in \mathrm{R}_+$

CHAPITRE XXV

VALEURS APPROCHÉES D'UN NOMBRE RÉEL

313. Valeurs approchées d'un nombre réel.

1° Soit un nombre réel défini par la section minorée ouverte α.

On considère :

$$\alpha_1 = \complement_Q \alpha.$$

α_1 est une section majorée. Si α_1 est ouverte, on pose $\alpha' = \alpha_1$. Si α_1 est fermée, on enlève la borne supérieure m et on pose : $\alpha' = \alpha_1 - \{ m \}$.

L'ensemble des deux sections ouvertes α et α' est une coupure.

2° ***Tout nombre rationnel a appartenant à α est une valeur rationnelle approchée de α par excès.***

Tout nombre rationnel a' appartenant à α' est une valeur rationnelle approchée de α par défaut.

On a évidemment :

$$a' < \alpha < a.$$

◇ *Exemple.*

Soit le nombre réel $\sqrt{2}$ défini par $\alpha = \{ x/x \in Q \quad \text{et} \quad 2 < x^2 \}$.

$a_1 = 2$ appartient à α; et 2 est une valeur approchée de $\sqrt{2}$ par excès.

$a'_1 = 1$ appartient à α'; et 1 est une valeur approchée de $\sqrt{2}$ par défaut

$a_2 = 1{,}5$ appartient à α, car $(1{,}5)^2 = 2{,}25$; et 1,5 est une valeur approchée de $\sqrt{2}$ par excès.

$a'_2 = 1{,}4$ appartient à α', car $(1{,}4)^2 = 1{,}96$; et 1,4 est une valeur approchée de $\sqrt{2}$ par défaut.

Donc :

$$1 < \sqrt{2} < 2$$
$$1{,}4 < \sqrt{2} < 1{,}5.$$

3° ***Deux valeurs approchées d'un nombre réel, l'un par défaut, l'autre par excès, constituent un encadrement du nombre réel.***

(1; 2) est un encadrement de $\sqrt{2}$ à une unité près.

(1,4; 1,5) est un encadrement de $\sqrt{2}$ à $\frac{1}{10}$ près.

314. Encadrements emboîtés.

Généralement on prend pour valeurs approchées a et a' des nombres décimaux de même ordre.

On a alors :

$$\frac{\lambda}{10^n} < \alpha < \frac{\lambda + 1}{10^n},$$

La différence des deux valeurs approchées $a' = \frac{\lambda}{10^n}$ et $a = \frac{\lambda + 1}{10^n}$ est $a - a' = \frac{1}{10^n}$.

On peut faire successivement $n = 1$, $n = 2$, ...

On obtient une suite croissante de valeurs approchées par défaut, et une suite décroissante de valeurs approchées par excès.

$$a'_1 < a'_2 < \ldots < a'_n < \ldots < \alpha < \ldots < a_n < \ldots < a_2 < a_1.$$

Les encadrements $(a'_1;\ a_1)$, $(a'_2;\ a_2)$, ... $(a'_n\ ;\ a_n)$ ... *sont des encadrements emboîtés (ou des intervalles emboîtés).*

La suite des amplitudes de ces intervalles emboîtés est

$$\frac{1}{10};\ \frac{1}{10^2};\ \ldots\ ;\ \frac{1}{10^n};\ \ldots$$

◇ *Exemple.*

Soit le nombre réel π. On a :

$$3{,}1 < \pi < 3{,}2 \quad \text{ou} \quad \frac{31}{10} < \pi < \frac{32}{10}$$

$$3{,}14 < \pi < 3{,}15 \quad \text{ou} \quad \frac{314}{100} < \pi < \frac{315}{100}$$

$$3{,}141 < \pi < 3{,}142 \quad \text{ou} \quad \frac{3\,141}{1\,000} < \pi < \frac{3\,142}{1\,000}$$

$$3{,}1415 < \pi < 3{,}1416 \quad \text{ou} \quad \frac{31\,415}{10\,000} < \pi < \frac{31\,416}{10\,000}$$

....

315. Expression décimale illimitée d'un nombre réel.

Soit un nombre réel quelconque α.

Les encadrements emboîtés permettent d'obtenir une suite croissante de valeurs approchées par défaut aussi précises qu'on le veut.

Par exemple, pour $\alpha = \sqrt{2}$, on a :

3,1
3,14
3,141
3,1415
.....

Le nombre α s'exprime alors sous forme décimale.

Plusieurs formes de développements décimaux sont possibles.

1° ***Le développement décimal est limité.***

Le nombre α est alors un nombre décimal rationnel.

Par exemple, si $\alpha = 2{,}32$ on a : $\alpha = \frac{232}{100}$.

D'autre part, on sait (cf. n° 271) que si le dénominateur d'une fraction irréductible ne contient que les facteurs premiers 2 et 5, le développement décimal est limité.

2° ***Le développement décimal est illimité périodique simple.***

a) Par exemple, soit α donné par

$$\alpha = 0{,}25\ 25\ 25...$$

25 est la période.

On a :

$$100\,\alpha = 25{,}25\ 25\ 25...$$

et

$$\alpha = 0{,}25\ 25\ 25...$$

D'où, par soustraction,

$$99\,\alpha = 25$$

et

$$\alpha = \frac{25}{99}$$

b) Le raisonnement précédent est général; et :

Si un nombre réel α a un développement décimal périodique simple, il est rationnel; et il s'exprime par une fraction ayant pour numérateur la période et pour dénominateur le nombre formé d'autant de 9 qu'il y a de chiffres dans la période.

c) Si le dénominateur d'une fraction irréductible ne contient aucun des facteurs premiers 2 et 5, le développement décimal est périodique.
On peut le vérifier, par exemple, en divisant 25 par 99.

3° *Le développement décimal est illimité périodique mixte.*

a) Par exemple, soit α donné par

$$\alpha = 0{,}315\,27\,27\,27\,\ldots$$

315 est la partie non périodique; 27 est la période.

On a :

$$100\,000\,\alpha = 31\,527{,}27\,27\,27\,\ldots$$

et

$$1\,000\,\alpha = \quad 315{,}27\,27\,27\,\ldots$$

D'où par soustraction

$$99\,000\,\alpha = 31\,527\text{-}315$$

et

$$\alpha = \frac{31\,527 - 315}{99\,000}$$

$$= \frac{31\,212}{99\,000}.$$

Le nombre α est donc rationnel.

b) Le raisonnement précédent est général; et :

Si un nombre réel α a un développement périodique mixte, il est rationnel ; et il s'exprime par une fraction ayant pour numérateur le nombre formé par la partie irrégulière et la période diminée du nombre formé par la partie irrégulière, et pour dénominateur le nombre formé d'autant de 9 qu'il y a de chiffres dans la période suivis d'autant de 0 qu'il y a de chiffres dans la partie irrégulière.

c) *Si le dénominateur d'une fraction irréductible contient avec d'autres facteurs premiers l'un, au moins, des facteurs premiers 2 et 5, le développement décimal illimité est périodique mixte.*
On peut le vérifier, par exemple, en divisant 31 212 par 99 000.

4° *Le développement décimal est illimité et non périodique.*

Dans ce cas le nombre α ne peut être un nombre rationnel, sinon le développement décimal serait limité (cf. 1°), ou illimité périodique simple (cf. 2°), ou illimité périodique mixte (cf. 3°) : α est donc irrationnel.
Si le développement décimal d'un nombre réel est illimité non périodique, ce nombre est irrationnel.
Par exemple, le nombre π est irrationnel.

316. Erreur absolue.

Soient le nombre réel α et les valeurs approchées a, par excès, et a', par défaut.

On considère les nombres

$$d = a - \alpha$$

et

$$d' = \alpha - a'$$

d est l'erreur absolue commise lorsqu'on remplace le nombre réel α par a.

d' est l'erreur absolue commise lorsqu'on remplace le nombre réel α par a'.

On désigne par $\Delta\alpha$ un majorant de d *et de* d' :

$$\Delta\alpha \geqslant \text{Sup}\,(d;\, d').$$

Dans la pratique, on ne connaît pas l'erreur absolue; sinon il serait possible de connaître excactement le nombre α. En général on connaît une valeur approchée a' par défaut, une valeur approchée a par excès et un majorant $\Delta\alpha$ des erreurs absolues. On a alors :

$$a' < \alpha < a' + \Delta\alpha$$

et

$$a - \Delta\alpha < \alpha < a.$$

Très souvent aussi on connaît une valeur approchée a'', sans savoir si elle est par défaut ou par excès; alors on a :

$$a'' - \Delta\alpha < \alpha < a'' + \Delta\alpha.$$

317. Erreur relative.

On appelle erreur relative commise lorsqu'on remplace α pa a le rapport :

$$\frac{\mathbf{d}}{\alpha} = \frac{\mathbf{a} - \alpha}{\alpha}.$$

On appelle erreur relative commise lorsqu'on remplace α par a' le rapport :

$$\frac{\mathbf{d}'}{\alpha} = \frac{\alpha - \mathbf{a}'}{\alpha}.$$

Les nombres d et d' sont inférieurs à $\Delta\alpha$. On obtient donc un majorant des deux erreurs relatives en remplaçant d et d' par $\Delta\alpha$:

$$\frac{d}{\alpha} < \frac{\Delta\alpha}{\alpha}$$

et

$$\frac{d'}{\alpha} < \frac{\Delta\alpha}{\alpha}.$$

On majore à nouveau $\frac{\Delta\alpha}{\alpha}$ en remplaçant α par la valeur approchée par défaut a' :

$$\frac{d}{\alpha} < \frac{\Delta\alpha}{a'}$$

et

$$\frac{d'}{\alpha} < \frac{\Delta\alpha}{a'}.$$

Donc :

$\frac{\Delta\alpha}{\mathbf{a}'}$ ***est un majorant des erreurs relatives.***

On pose :

$$r(\alpha) = \frac{\Delta\alpha}{a'} \qquad (317; 1)$$

et, par abus de langage, on appelle souvent $r(\alpha)$ *l'erreur relative commise sur* α.

318. Valeurs approchées d'une somme.

Soient les nombres réels α et β.

Si $\Delta\alpha$ est un majorant des erreurs absolues sur α, et $\Delta\beta$ un majorant des erreurs absolues sur β, et si a et b sont des valeurs approchées de α et β respectivement, on a :

$$a - \Delta\alpha < \alpha < a + \Delta\alpha$$

et

$$b - \Delta\beta < \beta < b + \Delta\beta.$$

D'où, par addition,

$$a + b - (\Delta\alpha + \Delta\beta) < \alpha + \beta < a + b + (\Delta\alpha + \Delta\beta).$$

Donc :

> $\mathbf{a} + \mathbf{b}$ ***est une valeur approchée de*** $\alpha + \beta$***, et*** $\Delta\alpha + \Delta\beta$ ***est un majorant des erreurs absolues commises en remplaçant*** $\alpha + \beta$ ***par*** $\mathbf{a} + \mathbf{b}$.

319. Valeurs approchées d'une différence.

Soient les nombres réels α et β.

Si $\Delta\alpha$ est un majorant des erreurs absolues sur α, et $\Delta\beta$ un majorant des erreurs absolues sur β, et si a et b sont des valeurs approchées de α et β respectivement, on a :

$$a - \Delta\alpha < \alpha < a + \Delta\alpha$$

et

$$b - \Delta\beta < \beta < b + \Delta\beta.$$

Le nombre $(a - \Delta\alpha) - (b + \Delta\beta)$ est une valeur approchée par défaut, et le nombre $(a + \Delta\alpha) - (b - \Delta\beta)$ est une valeur approchée par excès de $\alpha - \beta$. Et :

$$(a - \Delta\alpha) - (b + \Delta\beta) < \alpha - \beta < (a + \Delta\alpha) - (b - \Delta\beta)$$

ou

$$(a - b) - (\Delta\alpha + \Delta\beta) < \alpha - \beta < (a - b) + (\Delta\alpha + \Delta\beta).$$

Donc :

a — b *est une valeur approchée de* $\alpha - \beta$, *et* $\Delta\alpha + \Delta\beta$ *est un majorant des erreurs absolues commises en remplaçant* $\alpha - \beta$ *par* a — b.

320. Valeurs approchées d'un produit.

1° Soient les nombres réels positifs α et β.

Si $\Delta\alpha$ est un majorant des erreurs absolues sur α, et $\Delta\beta$ un majorant des erreurs absolues sur β, et si a et b sont des valeurs approchées de α et β respectivement, on a :

$$a - \Delta\alpha < \alpha < a + \Delta\alpha$$

et

$$b - \Delta\beta < \beta < b + \Delta\beta.$$

D'où :

$$(a - \Delta\alpha)\ (b - \Delta\beta) < \alpha\beta < (a + \Delta\alpha)\ (b + \Delta\beta)$$

ou

$$ab - (a\cdot\Delta\beta + b\cdot\Delta\alpha - \Delta\alpha\cdot\Delta\beta) < \alpha\beta < ab + (a\cdot\Delta\beta + b\cdot\Delta\alpha + \Delta\alpha\cdot\Delta\beta).$$

Donc :

ab *est une valeur approchée de* $\alpha\beta$, *et* a$\cdot\Delta\beta$ + b$\cdot\Delta\alpha + \Delta\alpha\cdot\Delta\beta$ *est un majorant des erreurs absolues commises en remplaçant* $\alpha\beta$ *par* ab.

On a encore :

$$a \cdot \Delta\beta + b \cdot \Delta\alpha + \Delta\alpha \cdot \Delta\beta < a \cdot \Delta\beta + b \cdot \Delta\alpha + 2 \cdot \Delta\alpha \cdot \Delta\beta$$

ou

$$a \cdot \Delta\beta + b \cdot \Delta\alpha + \Delta\alpha \cdot \Delta\beta < \Delta\alpha\ (b + \Delta\beta) + \Delta\beta\ (a + \Delta\alpha).$$

Si a'' et b'' sont des majorants de $a + \Delta\alpha$ et de $b + \Delta\beta$, le nombre $a'' \cdot \Delta\beta + b'' \cdot \Delta\alpha$ est un majorant des erreurs absolues commises en remplaçant $\alpha\beta$ par ab.

2° L'erreur relative sur le produit est majorée par

$$\frac{a \cdot \Delta\beta + b \cdot \Delta\alpha + \Delta\alpha \cdot \Delta\beta}{\alpha\beta} = \frac{\Delta\alpha \cdot (b - \Delta\beta) + \Delta\beta\,(a - \Delta\alpha) + 3 \cdot \Delta\alpha \cdot \Delta\beta}{\alpha \cdot \beta}.$$

En remplaçant α et β par leurs valeurs approchées par défaut, on majore à nouveau l'erreur relative par le nombre :

$$\frac{\Delta\alpha \cdot (b - \Delta\beta) + \Delta\beta \cdot (a - \Delta\alpha) + 3 \cdot \Delta\alpha \cdot \Delta\beta}{(a - \Delta\alpha)\,(b - \Delta\beta)}$$
$$= \frac{\Delta\alpha}{a - \Delta\alpha} + \frac{\Delta\beta}{b - \Delta\beta} + 3 \cdot \frac{\Delta\alpha}{a - \Delta\alpha} \cdot \frac{\Delta\beta}{b - \Delta\beta}.$$

Comme le produit $3 \cdot \frac{\Delta\alpha}{a - \Delta\alpha} \cdot \frac{\Delta\beta}{b - \Delta\beta}$ est très petit, dans la pratique on peut le négliger, et on prend comme erreur relative

$$\frac{\Delta\alpha}{a - \Delta\alpha} + \frac{\Delta\beta}{b - \Delta\beta}.$$

On a donc :

$$\mathbf{r}(\alpha \cdot \beta) = \mathbf{r}(\alpha) + \mathbf{r}(\beta). \qquad (320;\,1)$$

321. Valeurs approchées d'un quotient.

1° Soient les nombres réels positifs α et β.

Si $\Delta\alpha$ est un majorant des erreurs absolues sur α, et $\Delta\beta$ un majorant des erreurs absolues sur β, et si a et b sont des valeurs approchées de α et β respectivement, on a :

$$a - \Delta\alpha < \alpha < a + \Delta\alpha$$

et

$$b - \Delta\beta < \beta < b + \Delta\beta.$$

Le nombre $\frac{a - \Delta\alpha}{b + \Delta\beta}$ est une valeur approchée par défaut, et le nombre $\frac{a + \Delta\alpha}{b - \Delta\beta}$ est une valeur approchée par excès de $\frac{\alpha}{\beta}$.

Et :

$$\frac{a - \Delta\alpha}{b + \Delta\beta} < \frac{\alpha}{\beta} < \frac{a + \Delta\alpha}{b - \Delta\beta}.$$

D'autre part, si ΔQ est un majorant des erreurs absolues commises en remplacant $\varphi = \frac{\alpha}{\beta}$ par $\frac{a}{b}$, on a :

$$\frac{a}{b} - \Delta Q < \frac{\alpha}{\beta} < \frac{a}{b} + \Delta Q.$$

Donc :

$$2 \cdot \Delta Q = \frac{a + \Delta\alpha}{b - \Delta\beta} - \frac{a - \Delta\alpha}{b + \Delta\beta}$$

$$= \frac{ab + a \cdot \Delta\beta + b \cdot \Delta\alpha + \Delta\alpha \cdot \Delta\beta - ab + a \cdot \Delta\beta + b \cdot \Delta\alpha - \Delta\alpha \cdot \Delta\beta}{(b - \Delta\beta)\ (b + \Delta\beta)}$$

$$= 2 \cdot \frac{a \cdot \Delta\beta + b \cdot \Delta\alpha}{(b - \Delta\beta)\ (b + \Delta\beta)}.$$

D'où : $$\Delta Q = \frac{a \cdot \Delta\beta + b \cdot \Delta\alpha}{(b - \Delta\beta)\ (b + \Delta\beta)}.$$

Et :

$\frac{\mathrm{a}}{\mathrm{b}}$ est une valeur approchée de $\frac{\alpha}{\beta}$ et $\frac{\mathrm{a} \cdot \Delta\beta + \mathrm{b} \cdot \Delta\alpha}{(\mathrm{b} - \Delta\beta)\ (\mathrm{b} + \Delta\beta)}$ est un majorant des erreurs absolues commises en remplaçant $\frac{\alpha}{\beta}$ par $\frac{\mathrm{a}}{\mathrm{b}}$.

On peut majorer ΔQ en remplaçant $b + \Delta\beta$ par $b - \Delta\beta$. Et alors :

$\frac{a \cdot \Delta\beta + b \cdot \Delta\alpha}{(b - \Delta\beta)^2}$ est un majorant des erreurs absolues commises sur $\frac{\alpha}{\beta}$.

2° L'erreur relative sur le quotient est majorée par

$$\frac{a \cdot \Delta\beta + b \cdot \Delta\alpha}{(b - \Delta\beta)\ (b + \Delta\beta)} \cdot \frac{b + \Delta\beta}{a - \Delta\alpha} = \frac{a \cdot \Delta\beta + b \cdot \Delta\alpha}{(a - \Delta\alpha)\ (b - \Delta\beta)}$$

$$= \frac{\Delta\alpha \cdot (b - \Delta\beta) + \Delta\beta \cdot (a - \Delta\alpha) + 2 \cdot \Delta\alpha \cdot \Delta\beta}{(a - \Delta\alpha)\ (b - \Delta\beta)}$$

$$= \frac{\Delta\alpha}{a - \Delta\alpha} + \frac{\Delta\beta}{b - \Delta\beta} + 2 \cdot \frac{\Delta\alpha}{a - \Delta\alpha} \cdot \frac{\Delta\beta}{b - \Delta\beta}.$$

Comme le produit $2 \cdot \frac{\Delta\alpha}{a - \Delta\alpha} \cdot \frac{\Delta\beta}{b - \Delta\beta}$ est très petit, dans la pratique on peut le négliger, et on prend comme erreur relative

$$\frac{\Delta\alpha}{a - \Delta\alpha} + \frac{\Delta\beta}{b - \Delta\beta}.$$

On a donc :

$$r\left(\frac{\alpha}{\beta}\right) = r(\alpha) + r(\beta). \qquad (321 ; 1)$$

322. Calcul de la racine carrée d'un nombre réel positif.

On utilise la règle pratique suivante(1) :

Pour extraire la racine carrée d'un nombre :

1° On partage le nombre donné en tranches de deux chiffres à partir de la virgule, et de chaque côté de celle-ci.
La première tranche à gauche peut n'avoir qu'un chiffre.
Lorsque le nombre donné est un nombre décimal, si la dernière tranche à droite n'a qu'un chiffre on la complète avec un zéro.

2° On extrait la racine carrée de la première tranche à gauche. On obtient le premier chiffre de la racine et l'on soustrait de la première tranche le carré de ce chiffre. C'est le premier reste partiel.
A droite de ce reste, on abaisse la seconde tranche; on sépare par un point le dernier chiffre à droite.

3° On divise le nombre placé à gauche du point par le double du nombre trouvé à la racine. Le quotient est le deuxième chiffre de la racine ou un chiffre trop fort.
Il faut essayer ce chiffre; pour cela on l'écrit à la droite du double de la racine trouvée et on multiplie le nombre ainsi formé par le chiffre à essayer. Si ce produit se peut retrancher du premier reste partiel suivi de la deuxième tranche, le chiffre essayé est exact; sinon on essaye le chiffre immédiatement inférieur, jusqu'à ce que la soustraction soit possible. Le premier chiffre ainsi obtenu est le deuxième chiffre de la racine.
Le reste de la soustraction est le deuxième reste partiel.
A droite de ce reste, on abaisse la troisième tranche; on sépare par un point le dernier chiffre à droite.

4° On continue comme au 3°, jusqu'à ce qu'on ait abaissé toutes les tranches du nombre donné.

Si le nombre donné est décimal, on met une virgule à la racine avant d'abaisser la première tranche décimale. On continue ensuite comme si le nombre était entier.

---

(1) Rappel.

◇ *Exemple.*

Extraire la racine carrée de 525,367 *à* 0,01 *près.*

L'opération se dispose pratiquement de la façon suivante :

5 25,36 70	22,92
− 4	43 × 3 = 129
12.5	42 × 2 = 84
− 84	449 × 9 = 4 041
413.6	4 582 × 2 = 9 164.
− 40 41	
957,0	
− 9 164	
406	

La racine cherchée est 22,92 à 0,01 près par défaut.

CHAPITRE XXVI

LE CORPS C DES COMPLEXES

323. L'ensemble-produit $C = R^2$.

On considère l'ensemble $C = R^2$; c'est-à-dire l'ensemble des couples $\alpha = (a; b)$ formés de deux nombres réels. Après avoir introduit dans $C = R^2$, une addition et multiplication, les éléments de C seront appelés des *nombres complexes*. Par anticipation, les couples $\alpha = (a;b)$ sont appelés dès maintenant des nombres complexes.

Soient deux éléments $\alpha = (a; b)$ et $\alpha' = (a'; b')$; ces deux éléments sont égaux s'ils sont formés des mêmes nombres :

$$(\alpha = \alpha') \quad \Leftrightarrow \quad (a = a' \quad \text{et} \quad b = b').$$

324. Addition des nombres complexes.

Soient les deux nombres complexes

$$\alpha = (a; b) \quad \text{et} \quad \alpha' = (a'; b').$$

On définit une addition dans C par la formule

$$\alpha + \alpha' = (a; b) + (a'; b') = (a + a'; b + b').$$

◇ *Exemple.*

Soient $\alpha = (-2; 3)$ et $\alpha' = (4; -2)$. Calculer $\alpha + \alpha'$.

On a :

$$\alpha + \alpha' = (-2; 3) + (4; -2)$$
$$= (2; 1).$$

325. Propriétés de l'addition des complexes.

L'addition ainsi définie dans C possède les propriétés suivantes :

Commutativité.

Soient :

$$\alpha = (a; b) \quad \text{et} \quad \alpha' = (a'; b').$$

On a :

$$\alpha + \alpha' = (a + a'; b + b')$$

et

$$\alpha' + \alpha = (a' + a; b' + b).$$

Les résultats sont identiques.

Donc :

C $$(\forall\alpha)(\forall\alpha') \quad \alpha + \alpha' = \alpha' + \alpha.$$

Et :

L'addition des nombres complexes est commutative.

Associativité.

Soient :

$$\alpha = (a; b), \quad \alpha' = (a'; b'), \quad \alpha'' = (a''; b'')$$

On a :

$$\begin{aligned}(\alpha + \alpha') + \alpha'' &= (a + a'; b + b') + (a''; b'') \\ &= [(a + a') + a''; (b + b') + b'']\end{aligned}$$

et

$$\begin{aligned}\alpha + (\alpha' + \alpha'') &= (a; b) + (a' + a''; b' + b'') \\ &= [a + (a' + a''); b + (b' + b'')].\end{aligned}$$

Les deux résultats sont identiques.

Donc :

A $$(\forall\alpha)(\forall\alpha')(\forall\alpha'') : \quad (\alpha + \alpha') + \alpha'' = \alpha + (\alpha' + \alpha'').$$

Et :

L'addition des nombres complexes est associative.

Existence d'un élément neutre.

Soient :

$$\alpha = (a; b) \quad \text{et} \quad e = (0; 0).$$

On a :

$$\begin{aligned}\alpha + e &= (a + 0; b + 0) \\ &= \alpha.\end{aligned}$$

D'où, en tenant compte de la commutativité :

N $$(\forall\alpha) \quad \alpha + e = e + \alpha = \alpha.$$

Et :

Le complexe e = (0 ; 0) est neutre pour l'addition des complexes.

Au lieu de noter e = (0; 0) on note e = 0 puisque la loi est additive. Le neutre e = 0 est unique.

C est symétrisé pour l'addition.

Soit :

$$\alpha = (a; b).$$

On considère :

$$\alpha' = (-a; -b).$$

On a :

$$\begin{aligned}\alpha + \alpha' &= [a + (-a); b + (-b)]\\ &= (0; 0)\\ &= 0.\end{aligned}$$

D'où, en tenant compte de la commutativité :

$\boxed{S}$ $$(\forall\alpha)(\exists\alpha') : \quad \alpha + \alpha' = \alpha' + \alpha = 0.$$

Et :

Tous les nombres complexes ont un symétrique pour l'addition.

α' est l'opposé de α; on le note $\alpha' = -\alpha$.
Le symétrique $\alpha' = -\alpha$ est unique.

326. Groupe additif.

L'ensemble C des nombres complexes muni de l'addition précédente est un groupe, car l'addition possède les propriétés $\boxed{A}\boxed{N}\boxed{S}$.

De plus, l'addition possède la propriété $\boxed{C}$.

Donc :

Les nombres complexes forment un groupe additif commutatif.

On pose :

$$\boldsymbol{C}^* = \boldsymbol{C} - \{ 0 \}.$$

327. Régularité.

Soient trois nombres complexes α, β et μ.

On suppose que l'on a :

$$\alpha + \mu = \beta + \mu.$$

En ajoutant $-\mu$ aux deux membres de cette égalité, on obtient :

$$(\alpha + \mu) + (-\mu) = (\beta + \mu) + (-\mu)$$

ou

$$\alpha + [\mu + (-\mu)] = \beta + [\mu + (-\mu)]$$

ou

$$\alpha + 0 = \beta + 0$$

ou

$$\alpha = \beta.$$

Donc :

$$(\forall\alpha)\,(\forall\beta)\,(\forall\mu) : \quad \alpha + \mu = \beta + \mu \Rightarrow \alpha = \beta.$$

Et :

Tous les nombres complexes sont réguliers pour l'addition.

328. Soustraction.

Soient $\alpha \in \mathbf{C}$ ***et*** $\beta \in \mathbf{C}$.

Trouver un nombre complexe* x *tel que

$$\alpha = \beta + \mathbf{x}$$

s'appelle soustraire β ***de*** α.

En ajoutant $-\beta$ aux deux nombres de l'égalité précédente, on obtient :

$$\begin{aligned}(-\beta) + \alpha &= (-\beta) + \beta + x \\ &= 0 + x \\ &= x.\end{aligned}$$

Le nombre complexe x cherché est donc

$$x = \alpha + (-\beta).$$

Et :

Pour soustraire un nombre complexe, on ajoute son opposé.

Le nombre x est la différence entre α et β. On le note :

$$x = \alpha - \beta$$

D'où :

$$\alpha - \beta = \alpha + (-\beta).$$

329. Multiplication des nombres complexes.

Soient les deux nombres complexes :

$$\alpha = (\mathbf{a}\,;\mathbf{b}) \quad \text{et} \quad \alpha' = (\mathbf{a}'\,;\mathbf{b}').$$

On définit une multiplication dans C par la formule :

$$\alpha \cdot \alpha' = (\mathbf{aa' - bb' ; ab' + ba'}).$$

◇ *Exemple.*

Soient : $\alpha = (2; -1)$ et $\alpha' = (2; 3)$. Calculer $\alpha\alpha'$.

On a :

$$\begin{aligned}\alpha \cdot \alpha' &= (2; -1).(2; 3)\\ &= (4 + 3; 6 - 2)\\ &= (7; 4).\end{aligned}$$

330. Propriétés de la multiplication des complexes.

La multiplication ainsi définie dans C possède les propriétés suivantes :

Commutativité.

Soient :

$$\alpha = (a; b) \quad \text{et} \quad \alpha' = (a'; b')$$

On a :

$$\alpha \cdot \alpha' = (aa' - bb'; ab' + ba')$$

et

$$\alpha' \cdot \alpha = (a'a - b'b; a'b + b'a).$$

Les deux résultats sont identiques.

Donc :

C $$(\forall \alpha)\ (\forall \alpha') : \quad \alpha \cdot \alpha' = \alpha' \cdot \alpha.$$

Et :

La multiplication des nombres complexes est commutative.

Associativité.

Soient :

$$\alpha = (a; b), \quad \alpha' = (a'; b'), \quad \alpha'' = (a''; b'').$$

On a :

$$(\alpha\alpha')\,\alpha'' = (aa' - bb'; ab' + ba') \cdot (a''; b'')$$

$$= (aa'a'' - bb'a'' - ab'b'' - ba'b''; aa'b'' - bb'b'' + ab'a'' + ba'a'')$$

et

$$\alpha\,(\alpha'\alpha'') = (a; b)\,(a'a'' - b'b''; a'b'' + b'a'')$$

$$= (aa'a'' - ab'b'' - ba'b'' - bb'a''; aa'b'' + ab'a'' + ba'a'' - bb'b'')$$

Les deux résultats sont identiques.

Donc :

$\boxed{A}$ $$(\forall\alpha)\,(\forall\alpha')\,(\forall\alpha'') : \quad (\alpha\alpha')\,\alpha'' = \alpha\,(\alpha'\alpha'').$$

Et :

La multiplication des nombres complexes est associative.

Existence d'un élément neutre.

Soient :

$$\alpha = (a\,;b) \quad \text{et} \quad \varepsilon = (1\,;0).$$

On a :

$$\begin{aligned}\alpha \cdot \varepsilon &= (a\,;b)\cdot(1\,;0)\\ &= (a\,;b)\\ &= \alpha.\end{aligned}$$

D'où, en tenant compte de la commutativité :

$\boxed{N}$ $$(\forall\alpha) \quad \alpha\cdot\varepsilon = \varepsilon\cdot\alpha = \alpha.$$

Et :

Le complexe $\varepsilon = (1;0)$ est neutre pour la multiplication des complexes.

Au lieu de noter $\varepsilon = (1;\,0)$, on note $\varepsilon = 1$, puisque la loi est notée multiplicativement. Le neutre est unique.

C* est symétrisé pour la multiplication.

Soit le complexe non nul

$$\alpha = (a\,;b);$$

$\alpha \in C^*$. On considère :

$$\alpha' = \left(\frac{a}{a^2+b^2}\,;\frac{-b}{a^2+b^2}\right)$$

$a^2 + b^2 \neq 0$, puisque $\alpha \in C^*$.

On a :

$$\begin{aligned}\alpha\cdot\alpha' &= (a\,;b)\cdot\left(\frac{a}{a^2+b^2}\,;\frac{-b}{a^2+b^2}\right)\\ &= \left(\frac{a^2}{a^2+b^2}+\frac{b^2}{a^2+b^2}\,;\frac{-ab}{a^2+b^2}+\frac{ba}{a^2+b^2}\right)\\ &= (1\,;0)\\ &= 1.\end{aligned}$$

D'où, en tenant compte de la commutativité :

S $(\forall\alpha)\,(\exists\alpha') : \quad \alpha \cdot \alpha' = \alpha' \cdot \alpha = 1.$

Et :

Tous les nombres complexes, non nuls, ont un symétrique pour la multiplication.

α' est l'inverse de α; on le note : $\alpha' = \alpha^{-1}$.

331. Groupe multiplicatif.

L'ensemble $C^* = C - \{0\}$ est muni d'une multiplication possédant les propriétés A N S C.

Donc :

Les nombres complexes, non nuls, forment un groupe multiplicatif commutatif.

332. Régularité.

Soient les trois nombres complexes α, β, μ ($\alpha \in C$; $\beta \in C$; $\mu \in C^*$).

On suppose que l'on a :

$$\alpha\mu = \beta\mu.$$

En multipliant par μ^{-1} les deux membres de cette égalité, on obtient :

$$(\alpha\mu)\mu^{-1} = (\beta\mu)\mu^{-1}$$

ou

$$\alpha(\mu \cdot \mu^{-1}) = \beta \cdot (\mu \cdot \mu^{-1})$$

$$\alpha \times 1 = \beta \times 1$$

ou

$$\alpha = \beta.$$

Donc :

$$(\forall\alpha)\,(\alpha \in C)\,(\forall\beta)\,(\beta \in C)\,(\forall\mu)\,(\mu \in C^*) : \quad \alpha\mu = \beta\mu \Rightarrow \alpha = \beta.$$

Et :

Tous les complexes, non nuls, sont réguliers pour la multiplication.

333. Division.

Soient $\alpha \in C$ et $\beta \in C^*$.
Trouver un nombre complexe $\mathbf{x}$, $(\mathbf{x} \in C)$, tel que

$$\alpha = \beta \cdot \mathbf{x}$$

s'appelle diviser α par β.

En multipliant les deux membres de l'égalité précédente par β^{-1}, on a :

$$\begin{aligned}\beta^{-1}\cdot\alpha &= \beta^{-1}(\beta x)\\ &= (\beta^{-1}\cdot\beta)\cdot x\\ &= 1.x\\ &= x.\end{aligned}$$

Le nombre x cherché est donc :

Et : $$x = \alpha\cdot\beta^{-1}.$$

Pour diviser par un nombre complexe, on multiplie par son inverse.

On note : $x = \dfrac{\alpha}{\beta}$

et

$$x = \alpha \times \frac{1}{\beta}.$$

334. Distributivité de la multiplication pour l'addition.

Soient les nombres complexes :

$$\alpha = (a;b),\quad \alpha' = (a';b'),\quad \mu = (p;q)$$

On a :

$$\begin{aligned}\mu(\alpha+\alpha') &= (p;q)\cdot(a+a';b+b')\\ &= (pa+pa'-qb-qb';pb+pb'+qa+qa')\end{aligned}$$

et

$$\begin{aligned}\mu\alpha+\mu\alpha' &= (pa-qb;pb+qa)+(pa'-qb';pb'+qa')\\ &= (pa-qb+pa'-qb';pb+qa+pb'+qa').\end{aligned}$$

Les deux résultats sont identiques.

Donc :

[D] $(\forall\alpha)(\forall\alpha')(\forall\mu)$: $\mu(\alpha+\alpha') = \mu\alpha+\mu\alpha'$

$(\alpha+\alpha')\mu = \alpha\mu+\alpha'\mu.$

Et :

La multiplication des complexes est distributive pour l'addition des complexes.

335. Le corps C des complexes.

L'ensemble C des nombres complexes est muni d'une loi de composition interne, notée additivement, et douant C d'une structure de groupe commutatif, c'est-à-dire possédant les propriétés [A] [N] [S] [C].

L'ensemble C est muni d'une seconde loi de composition interne, notée multiplicativement, et douant C* d'une structure de groupe commutatif, c'est-à-dire possédant les propriétés $\boxed{A}\boxed{N}\boxed{S}\boxed{C}$.
De plus, la multiplication est distributive pour l'addition.

Ainsi :

C est le corps commutatif des complexes.

336. Plongement de R dans C.

Soit C′ l'ensemble des complexes de la forme $(m;\,0)$.
On peut envisager l'application φ qui à $m \in \mathrm{R}$ fait correspondre $(m;\,0) \in \mathrm{C}'$:

$$\varphi : \qquad m \in \mathrm{R} \longrightarrow \varphi(m) = (m;0) \in \mathrm{C}'$$

Cette application est manifestement bijective.

De plus, on a :

$$\begin{aligned}\varphi(m+m') &= (m+m';0)\\ &= (m;0)+(m';0)\end{aligned}$$

ou

$$\varphi(m+m') = \varphi(m)+\varphi(m')$$

et

$$\begin{aligned}\varphi(mm') &= (mm';0)\\ &= (m;0)\cdot(m';0)\end{aligned}$$

ou

$$\varphi(mm') = \varphi(m)\cdot\varphi(m').$$

Et :

L'application φ respecte l'addition et la multiplication.

Il est donc possible d'identifier m et $(m;\,0)$, c'est-à-dire d'identifier R et C′. On a alors plongé, ou immergé, R dans C.

Ainsi :

Le corps R est un sous-corps du corps C.

On a :

$$\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}.$$

Cette suite d'inclusions met bien en évidence les extensions successives de la notion de nombre et la construction progressive des nombres.

337. Multiplication d'un nombre complexe par un nombre réel.

1° ***Soient un nombre réel* m *et un nombre complexe* $\alpha = (a; b)$. *On définit une loi de composition externe par :***

$$(m;\alpha) \in R \times C \longrightarrow m \cdot \alpha = (ma; mb) \in C.$$

2° *m* étant un réel est identique au complexe $(m; 0)$. On a alors :

$$m \cdot \alpha = (m; 0) \cdot (a; b) = (ma; mb).$$

Il n'y a pas de contradiction entre la multiplication des complexes et la multiplication d'un nombre complexe par un réel.

3° La multiplication d'un complexe et d'un réel, étant un cas particulier de la multiplication des complexes, possède les propriétés suivantes :

D' $(\forall m)\ (\forall \alpha)\ (\forall \beta)$: $m(\alpha + \beta) = m\alpha + m\beta.$

D'' $(\forall m)\ (\forall p)\ (\forall \alpha)$: $(m + p)\,\alpha = m\alpha + p\alpha.$

N' $(\forall \alpha)$: $1 \times \alpha = \alpha.$

A' $(\forall m)\ (\forall p)\ (\forall \alpha)$: $m\,(p\alpha) = (mp) \cdot \alpha.$

◇ *Exemples :*

$$2 \cdot (3; 1) = (6; 2)$$
$$a \cdot (1; 0) = (a; 0)$$
$$b \cdot (0; 1) = (0; b).$$

338. Le nombre *i*.

On considère le nombre complexe :

$$i = (0; 1).$$

On a :

$$i^2 = (0; 1) \cdot (0; 1) = (-1; 0)$$

ou

$$\mathbf{i^2 = -1.}$$

D'où :

$$\mathbf{i^3 = -i}$$

et

$$\mathbf{i^4 = 1.}$$

De $i^2 = -1$, on déduit :

$$\frac{1}{i} = -i.$$

339. Expression cartésienne d'un nombre complexe.

Soit le nombre complexe $\alpha = (a; b)$. On a :

$$\begin{aligned} \alpha &= (a; b) \\ &= (a; 0) + (0; b) \\ &= a \cdot (1; 0) + b \cdot (0; 1) \\ &= a \times 1 + bi \\ &= a + bi. \end{aligned}$$

Donc :

$$\alpha = \mathbf{(a; b) = a + bi.}$$

Le nombre a *est la partie réelle de* α; *et on écrit :*

$$\Re e(\alpha) = \mathrm{a}.$$

Le nombre b *est la partie imaginaire de* α; *et on écrit :*

$$\Im m\ (\alpha) = \mathrm{b}.$$

340. Utilisation de l'expression cartésienne dans les opérations.

1° Soient les nombres complexes

$$\alpha = a + bi \quad \text{et} \quad \alpha' = a' + b'i.$$

On a :

$$\begin{aligned} \alpha + \alpha' &= a + bi + a' + b'i \\ &= (a + a') + (b + b')i \\ &= (a + a'; b + b') \end{aligned}$$

et

$$\begin{aligned} \alpha\alpha' &= (a + bi)(a' + b'i) \\ &= aa' + ab'i + ba'i + bb'i^2 \\ &= (aa' - bb') + (ab' + ba')i \\ &= (aa' - bb'; ab' + ba'). \end{aligned}$$

On peut donc effectuer les additions et les multiplications de nombres complexes en utilisant les propriétés du corps commutatif et les expressions cartésiennes à condition de remplacer $\mathbf{i^2}$ ***par*** $\mathbf{-1}$ ***chaque fois que cela est possible.***

2° Soit le nombre complexe

$$\alpha = a + bi.$$

On a :

$$\begin{aligned} \alpha \cdot (a - bi) &= (a + bi)(a - bi) \\ &= a^2 + b^2 \end{aligned}$$

ou

$$\alpha \cdot \left[\frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}\, i\right] = 1$$

et par suite :

$$\alpha^{-1} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}\, i$$

$$\alpha^{-1} = \left(\frac{a}{a^2 + b^2}; \frac{-b}{a^2 + b^2}\right).$$

On retrouve ainsi la formule donnée arbitrairement au n° 330 pour l'inverse de α.

341. Nombres complexes conjugués.

1° Soit un nombre complexe $\alpha = a + bi$.

Le nombre complexe $a - bi$ est appelé le complexe conjugué de $\alpha = a + bi$.

On le note :

$$\bar{\mathbf{a}} = \mathbf{a} - \mathbf{bi}$$

et on lit « *a barre* ».

2° On a immédiatement :

$$\bar{\mathbf{i}} = -\mathbf{i} \quad \textbf{et} \quad \bar{0} = 0$$

et

$$\bar{\bar{\alpha}} = \alpha.$$

3° On a aussi :

$$\alpha + \bar{\alpha} = a + bi + a - bi$$

ou

$$\alpha + \bar{\alpha} = 2a$$

et

$$\alpha\bar{\alpha} = (a + bi)\,(a - bi)$$

ou

$$\alpha\bar{\alpha} = \mathbf{a}^2 + \mathbf{b}^2.$$

4° Soient deux nombres complexes :

$$\alpha = a + bi, \quad \alpha' = a' + b'i,$$

leur somme et leur produit :

$$\alpha + \alpha' = (a + a') + (b + b')i$$
$$\alpha\alpha' = (aa' - bb') + (ab' + ba')i$$

D'où :

$$\overline{\alpha + \alpha'} = (a + a') - (b + b')\,i$$
$$= (a - bi) + (a' - b'i)$$

et

$$\overline{\alpha + \alpha'} = \bar{\alpha} + \overline{\alpha'}.$$

De même :

$$\overline{\alpha\alpha'} = (aa' - bb') - (ab' + ba')\,i$$
$$= (a - bi)\;(a' - b'i)$$

et

$$\overline{\alpha\alpha'} = \bar{\alpha} \cdot \overline{\alpha'}.$$

5° On a encore (cf n° 340) :

$$\frac{1}{\alpha} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\,i$$

D'où :

$$\overline{\left(\frac{1}{\alpha}\right)} = \frac{a}{a^2 + b^2} + \frac{b}{a^2 + b^2}\,i.$$

D'autre part :

$$\frac{1}{\bar{\alpha}} = \frac{1}{a - bi}$$
$$= \frac{a + bi}{(a - bi)\;(a + bi)}$$
$$= \frac{a + bi}{a^2 + b^2}.$$

Donc :

$$\overline{\left(\frac{1}{\alpha}\right)} = \frac{1}{\bar{\alpha}}.$$

342. Valeur absolue d'un nombre complexe.

1° Soit $\alpha \in C$. On définit une application de C dans R_+ par :

v : $\qquad \alpha \in C \longrightarrow v(\alpha) = \sqrt{a^2 + b^2} \in R_+$

$v(\alpha)$ est la valeur absolue de α; on note $v(\alpha) = |\alpha|$

Donc :

$$|\alpha| = \sqrt{\mathbf{a^2 + b^2}}$$

ou

$$|\alpha| = \sqrt{\alpha \cdot \bar{\alpha}}$$

2° On a immédiatemment :

$$|-\alpha| = |\alpha|$$

et

$$|\alpha| = 0 \Leftrightarrow \alpha = 0$$

et encore

$$|\alpha| = |\bar{\alpha}|.$$

3° On a :

$$|\mathfrak{Re}(\alpha)| \leqslant |\alpha|, \quad \text{car} \quad |a| \leqslant \sqrt{a^2+b^2}$$

et

$$|\mathfrak{Im}(\alpha)| \leqslant |\alpha|, \quad \text{car} \quad |b| \leqslant \sqrt{a^2+b^2}.$$

4° On a aussi :

$$|\alpha|^2 = a^2 + b^2$$

ou

$$|\alpha|^2 = \alpha \cdot \bar{\alpha}.$$

343. Valeur absolue du produit de deux complexes.

Soient les nombres complexes α et α'; on a :

$$\begin{aligned} |\alpha \cdot \alpha'|^2 &= (\alpha\alpha') \cdot \overline{(\alpha\alpha')} \\ &= (\alpha\alpha') \cdot (\bar{\alpha} \cdot \bar{\alpha}') \\ &= (\alpha\bar{\alpha}) \times (\bar{\alpha}'\alpha') \\ &= |\alpha|^2 \cdot |\alpha'|^2. \end{aligned}$$

D'où :

$$|\alpha\alpha'| = |\alpha| \cdot |\alpha'|.$$

344. Valeurs absolues d'une somme et d'une différence de complexes.

1° Soient les nombres complexes α et α'; on a

$$\begin{aligned} |\alpha + \alpha'|^2 &= (\alpha + \alpha') \cdot \overline{(\alpha + \alpha')} \\ &= (\alpha + \alpha') \cdot (\bar{\alpha} + \bar{\alpha}') \\ &= \alpha\bar{\alpha} + \alpha\bar{\alpha}' + \alpha'\bar{\alpha} + \alpha'\bar{\alpha}' \\ &= |\alpha|^2 + |\alpha'|^2 + \alpha\bar{\alpha}' + \alpha'\bar{\alpha}. \end{aligned}$$

Or, en posant $\alpha = a + bi$ et $\alpha' = a' + b'i$, on a :

$$\begin{aligned} \alpha\bar{\alpha}' &= (a + bi)\,(a' - b'i) \\ &= aa' + bb' + (-ab' + ba')i \end{aligned}$$

et

$$\alpha'\bar{\alpha} = (a' + b'i)(a - bi)$$
$$= (aa' + bb') + (ab' - ba')i.$$

D'où :

$$\alpha\overline{\alpha'} + \alpha'\bar{\alpha} = 2\,(aa' + bb')$$
$$= 2 \cdot \mathcal{R}e\,(\alpha\overline{\alpha'}) = 2\,\mathcal{R}e\,(\bar{\alpha}\alpha')$$

Or

$$|\,\mathcal{R}e\,(\alpha\overline{\alpha'})\,| \leqslant |\,\alpha\overline{\alpha'}\,|$$

On a donc, puisque $|\,\alpha\overline{\alpha'}\,| = |\,\alpha\,| \cdot |\,\overline{\alpha'}\,| = |\,\alpha\,| \cdot |\,\alpha'\,|$

$$|\alpha|^2 + |\alpha'|^2 - 2 \cdot |\alpha| \cdot |\alpha'| \leqslant |\alpha + \alpha'|^2 \leqslant |\alpha|^2 + |\alpha'|^2 + 2|\alpha| \cdot |\alpha'|$$

ou

$$\big||\alpha| - |\alpha'|\big|^2 \leqslant |\alpha + \alpha'|^2 \leqslant (|\alpha| + |\alpha'|)^2$$

ou finalement :

$$\big||\alpha| - |\alpha'|\big| \leqslant |\alpha + \alpha'| \leqslant |\alpha| + |\alpha'|.$$

2° En remarquant que

$$\alpha - \alpha' = \alpha + (-\alpha')$$

on déduit de l'inégalité précédente

$$\big||\alpha| - |\alpha'|\big| \leqslant |\alpha - \alpha'| \leqslant |\alpha| + |\alpha'|.$$

CHAPITRE XXVII

PROGRESSIONS

345. Suites numériques.

1° Soit l'ensemble $I = \{1; 2; 3; ...; n\}$.

On considère l'application u :

$$u : \quad k \in I \longrightarrow u(k) = u_k \in C.$$

L'ensemble ordonné :

$$u_1 \quad u_2 \quad u_3 \quad \dots \quad u_n$$

est une suite de nombres. Les nombres u_1, u_2, u_3, ..., u_n sont les termes de la suite, n est le nombre de termes.

2° ***Une suite peut être déterminée par son premier terme et par la donnée d'un terme quelconque en fonction du terme précédent, c'est-à-dire par u_1 et la formule***

$$u_{k+1} = f(u_k).$$

La suite est dite déterminée par récurrence.

◇ *Exemple.*

a) $u_1 = 1 \qquad u_{k+1} = 2u_k - 3.$

b) $u_1 = 3$ et $u_{k+1} = \dfrac{u_k + 2}{u_k - 2}.$

3° On pose :

$$S_n = u_1 + u_2 + ... + u_n$$

S_n est la somme des n termes de la suite.

4° *On suppose maintenant que la suite est une suite de nombres réels.*

Si on a :

$$(\forall k) \quad u_k < u_{k+1}$$

on dit que la suite est croissante; l'application u est, en effet, une application croissante.

Si on a :

$$(\forall k) \quad u_k > u_{k+1}$$

on dit que la suite est décroissante; l'application u est une application décroissante.

346. Progression arithmétique.

1° ***On appelle progression arithmétique la suite de*** $\mathbf{n}$ ***nombres déterminée par le premier terme*** $\mathbf{u_1 = a}$ ***et la formule de récurrence***

$$\mathbf{u_{k+1} = u_k + r,}$$

$\mathbf{r}$ ***étant un nombre constant appelé raison.***

◇ *Exemples.*

$u_1 = 2,\quad u_2 = 5,\quad u_3 = 8,\quad u_4 = 11 \qquad (r = 3)$

$u_1 = 7,\quad u_2 = 3,\quad u_3 = -1,\quad u_4 = -5;\quad u_5 = -9 \qquad (r = -4)$

2° *En renversant l'ordre, des termes d'une progression arithmétique, on obtient une nouvelle progression arithmétique ayant pour raison l'opposée de la raison de la première progression.*

◇ *Exemple.*

Soit la progression arithmétique de raison 2

$$u_1 = 1 \quad u_2 = 3 \quad u_3 = 5 \quad u_4 = 7.$$

En renversant l'ordre des termes, on obtient une nouvelle progression arithmétique :

$$v_1 = 7 \quad v_2 = 5 \quad v_3 = 3 \quad v_4 = 1$$

dont la raison est — 2.

3° Soit la progression arithmétique de n termes, de premier terme $u_1 = a$ et de raison r. On a :

$$u_1 = a$$
$$u_2 = a + r$$
$$u_3 = a + 2r$$
$$\dots\dots\dots\dots\dots\dots$$
$$u_k = a + (k-1)r$$
$$\dots\dots\dots\dots\dots\dots$$
$$u_n = a + (n-1)r$$

La formule :

$$\mathbf{u_k = a + (k-1)r}$$

donne la valeur d'un terme en fonction de son rang. Ce n'est donc plus une formule de récurrence qui détermine les termes de la progression.

4° *On suppose maintenant que la suite est une suite de nombres réels.*

Si la raison est positive, la progression est croissante.
Si la raison est négative, la progression est décroissante.

347. Somme de deux termes équidistants des termes extrêmes d'une progression arithmétique.

Les deux termes u_k *et* u_{n-k+1} *sont dits équidistants des extrêmes;* le nombre de termes précédant u_k est $k - 1$; le nombre de termes suivant u_{n-k+1} est aussi $k - 1$.

On a :

$$u_k = a + (k - 1)r$$

et

$$u_{n-k+1} = a + (n - k)r$$

Par suite :

$$u_k + u_{n-k+1} = 2a + (n - 1)r$$
$$= a + [a + (n - 1)r]$$

ou

$$\mathbf{u}_k + \mathbf{u}_{n-k+1} = \mathbf{u}_1 + \mathbf{u}_n.$$

Donc :

Dans une progression arithmétique, la somme de deux termes équidistants des extrêmes est égale à la somme des extrêmes.

Remarque

Si le nombre des termes est impair, $n = 2p + 1$, il y a un terme central $u_k = u_{p+1}$.

Or :

$$n - k + 1 = 2p + 1 - p - 1 + 1 = p + 1.$$

Donc :

$$u_k = u_{n-k+1}.$$

Et alors :

$$2\,u_{p+1} = u_1 + u_{2p+1}.$$

348. Somme des termes d'une progression arithmétique.

On a :

$$S_n = u_1 + u_2 + \dots + u_{n-1} + u_n$$

et

$$S_n = u_n + u_{n-1} + \dots + u_2 + u_1.$$

D'où :

$$2.\ S_n = (u_1 + u_n) + (u_2 + {}_{n-1}) + \dots + (u_{n-1} + u_2) + (u_n + u_1) = n \cdot (u_1 + u_n)$$

et

$$S_n = \frac{\mathbf{n\ (u_1 + u_n)}}{\mathbf{2}} \qquad (348;\ 1)$$

Or :

$$u_1 + u_n = 2a + (n - 1)r$$

et :

$$S_n = \frac{\mathbf{n\,[2\,a + (n - 1)\,r]}}{\mathbf{2}}. \qquad (348;\ 2)$$

◇ *Exemple 1.*

Calculer la somme des n premiers nombres entiers.

Les n premiers nombres entiers forment une progression arithmétique de n termes avec $u_1 = 1$ et $r = 1$. On a : $u_n = n$.

La formule (348;1), donne :

$$S_n = \frac{\mathbf{n\ (n + 1)}}{\mathbf{2}}.$$

◇ *Exemple 2.*

Calculer la somme des n premiers nombres impairs.

Les n premiers nombres impairs forment une progression arithmétique de n termes avec $u_1 = 1$ et $r = 2$. On a : $u_n = 2n - 1$.

La formule (348;1) donne

$$S_n = \frac{n \cdot 2n}{2}$$

ou

$$S_n = n^2.$$

349. Progression géométrique.

1° *On appelle progression géométrique la suite de* n *nombres déterminée par le premier terme* $u_1 = a$ *et la formule de récurrence*

$$\mathbf{u_{k+1} = q \cdot u_k},$$

q *étant un nombre constant appelé raison.*

◇ *Exemples.*

$$u_1 = \frac{3}{2}, \quad u_2 = 3, \quad u_3 = 6 \quad u_4 = 12 \quad (q = 2)$$

$$v_1 = -\frac{3}{2} \quad v_2 = 3 \quad v_3 = -6 \quad v_4 = 12 \quad (q = -2)$$

2° *En renversant l'ordre des termes d'une progression géométrique, on obtient une nouvelle progression géométrique ayant pour raison l'inverse de la raison de la première progression.*

◇ *Exemple.*

Soit la progression géométrique de raison $-\frac{3}{2}$:

$$u_1 = 1, \quad u_2 = -\frac{3}{2}, \quad u_3 = \frac{9}{4}; \quad u_4 = -\frac{27}{8}; \quad u_5 = \frac{81}{16}.$$

En renversant l'ordre des termes, on obtient une nouvelle progression géométrique :

$$v_1 = \frac{81}{16}, \quad v_2 = -\frac{27}{8}, \quad v_3 = \frac{9}{4}, \quad v_4 = -\frac{3}{2}; \quad v_5 = +1$$

dont la raison est $-\frac{2}{3}$.

3° Soit la progression géométrique de n termes, de premier terme $u_1 = a$ et de raison q. On a :

$$\begin{aligned} u_1 &= a \\ u_2 &= aq \\ u_3 &= aq^2 \\ &\dots\dots \\ u_k &= aq^{k-1} \\ &\dots\dots \\ u_n &= aq^{n-1} \end{aligned}$$

La formule

$$\mathbf{u}_k = \mathbf{a} \cdot \mathbf{q}^{k-1}$$

donne la valeur d'un terme en fonction de son rang. Ce n'est donc plus une formule de récurrence qui détermine les termes de la progression.

4° *On suppose maintenant que la suite est une suite de nombres réels.*

Si la raison est positive, tous les termes sont de même signe.

Si la raison est négative, les termes sont alternativement positifs et négatifs.

350. Somme des termes d'une progression géométrique.

On a :

$$S_n = u_1 + u_2 + \ldots + u_{n-1} + u_n$$

et

$$q \cdot S_n = q \cdot u_1 + q \cdot u_2 + \ldots + q \cdot u_{n-1} + qu_n$$
$$= u_2 + u_3 + \ldots + u_n + qu_n$$

D'où :

$$(q - 1) S_n = q \cdot u_n - u_1$$
$$= aq^n - a.$$

Si q est différent de 1, on a :

$$S_n = \frac{aq^n - a}{q - 1} \qquad (350;1)$$

$$S_n = \frac{a(q^n - 1)}{q - 1} \qquad (350;2)$$

$$S_n = \frac{qu_n - u_1}{q - 1} \qquad (350;3)$$

Si q est égal à 1, on a :

$$u_1 = u_2 = \ldots = u_n = a$$

et

$$S_n = na. \qquad (350;4)$$

◇ *Exemple.*

Calculer la somme des termes de la progression géométrique

$$u_1 = \frac{3}{2}, \quad u_2 = 3, \quad u_3 = 6, \quad u_4 = 12, \quad u_5 = 24.$$

Le premier terme est $u_1 = a = \frac{3}{2}$ et la raison est $q = 2$. La formule (350;2) donne :

$$S_5 = \frac{\frac{3}{2}(2^5 - 1)}{2 - 1}$$
$$= \frac{3}{2} \times (2^5 - 1)$$
$$= \frac{3}{2} \times 31$$

et finalement:

$$S_5 = \frac{93}{2}.$$

EXERCICES ET PROBLÈMES SUR LE LIVRE II.

Lois de composition.

77. Dans N, on considère la loi de composition interne définie par

$$x \star y = x + 2y$$

Cette loi est-elle commutative ? Est-elle associative ?

78. Dans Z, on considère la loi interne définie par

$$x \top y = 2x + 3y.$$

Cette loi est-elle associative ? commutative ? Y a-t-il un élément neutre ?

79. Dans l'ensemble Q des nombres rationnels, on considère la loi interne

$$x \perp y = \frac{2x + y}{3}.$$

Est-elle associative ? commutative ?

80. Dans N, on considère l'addition, notée +, et la loi interne

$$x \star y = x + 2y.$$

L'opération $\ast$ est-elle distributive pour l'addition ?
L'addition est-elle distributive pour la loi $\ast$?

81. Soit dans N la loi

$$x \perp y = 2x + y.$$

Examiner s'il existe des éléments neutres.
Y a-t-il des éléments réguliers à droite ? à gauche ?

82. Dans Z, on considère la loi

$$x \top y = x + y^2.$$

Quelles sont les propriétés de cette loi ? Y a-t-il des éléments neutres ?

83. Dans N, soit la loi

$$x \star y = x^2 + y^2.$$

Étudier l'associativité, la commutativité, l'existence d'un élément neutre.

84. Dans N, on considère la loi

$$x \top y = x + y + 2xy.$$

Cette loi est-elle commutative ? associative ?
Rechercher s'il existe des éléments neutres.
Y a-t-il des éléments réguliers ?

85. Soit dans Z, la loi

$$a \star b = 2ab.$$

Quelles en sont les propriétés.
La loi $\star$ est-elle distributive pour l'addition dans Z ; pour la multiplication dans Z ?

86. Dans N, étudier la oi

$$x \top y = x^2 y^2.$$

87. Étudier la loi interne, dans Z :

$$x \perp y = x.$$

88. Dans Q, on envisage la loi

$$x \ast y = x + \frac{1}{y}.$$

Étudier cette loi.

89. Dans Z, on envisage la loi

$$x \ast y = x + y + xy.$$

1° Étudier les propriétés de cette loi.
2° Est-elle distributive pour l'addition dans Z ? pour la multiplication dans Z ?
3° Quels sont les éléments symétrisables ?

90. Dans Q^2, on considère les éléments $\alpha = (a; b)$, $\alpha' = (a'; b')$, $\alpha'' = (a''; b'')$... et on introduit la loi

$$\alpha \star \alpha' = (a ; b) \star (a' ; b') = (aa' ; ba' + b')$$

Étudier la commutativité et l'associativité.
Déterminer l'élément neutre.
Éléments inversibles.

91. Dans Z^2, on introduit les deux lois internes

$$(a; b) + (a'; b') = (a + a'; b + b')$$

et

$$(a; b) \cdot (a'; b') = (aa' - bb'; ab' + ab')$$

Étudier les propriétés de ces deux lois.
La seconde est-elle distributive pour la première ?

92. Dans Z^2, on introduit les deux lois internes :

$$(a; b) + (a'; b') = (a + a'; b + b')$$

et

$$(a; b) . (a'; b') = (aa'; ab' + ba').$$

Étudier ces deux lois. Distributivité.

93. Soit l'ensemble $E = Z^2$. On envisage l'application f de $Z \times E$ sur E définie par

$$f : [\alpha ; (a ; b)] \in Z \times E \longrightarrow f[\alpha ; (a ; b)] = \alpha (a ; b) = (\alpha a ; \alpha b) \in E.$$

Montrer que f est une loi externe. Quelles sont les propriétés de cette loi ?

94. Soit l'ensemble $E = Q^2$. On considère la loi interne

$$(a; b) + (a'; b') = (a + a'; b + b')$$

et la loi externe

$$\alpha (a ; b) = (\alpha a ; 0) \qquad (\alpha \in Q).$$

Quelles sont les propriétés de ces deux lois ? Relations entre ces lois ?

Nombres naturels.

95. Trouver les nombres de N tels que $a + b = ab$.

96. Soit $A \in N$ un nombre de trois chiffres représenté par $A = \overline{cdu}$. On demande de déterminer A sachant que

$$\begin{cases} 3c + d + u = \overline{ud} + 9 \\ \overline{cdu} = \overline{cud} + 27 \\ 7 \mid \overline{cdu} \quad \text{et} \quad 7 \mid \overline{udc} \end{cases}$$

97. Trouver un nombre $A = \overline{cdu}$ sachant que

$$c + d + u = \overline{ud} + 1$$
$$10c + \overline{cu} = \overline{du}.$$

98. Déterminer les nombres A et B sachant que leur différence est 8, et que si on augmente ces deux nombres de 2 leur produit augmente de 72.

99. Montrer que les deux assertions :
a) le quotient d'une division ne change pas quand on augmente le diviseur de une unité;
b) le reste d'une division est au moins égal au quotient;
sont équivalentes.

100. En divisant le nombre $A = 2103$ par le nombre B on trouve 81 pour reste. Déterminer B et Q ($A = BQ + R$).

101. Résoudre dans N l'équation

$$x + 5y = 38.$$

102. Trouver deux nombres sachant que leur somme est 289, et que si on divise le plus grand par le plus petit on obtient 16 pour quotient.

103. Soient les nombres $A = \overline{du}$ et $A' = \overline{ud}$ $(d > u)$.
1° Montrer que

$$A - A' = 9(d - u).$$

2° Déterminer le nombre A sachant que la somme de ses chiffres est 15 et que la différence $A - A'$ est 27.

104. Soient les deux nombres $A = \overline{cdu}$ et $A' = \overline{udc}$ avec $c > u$.
1° Montrer :

$$A - A' = \overline{\gamma\beta\alpha} \quad \Rightarrow \quad \beta = 9 \quad \text{et} \quad \alpha + \gamma = 9.$$

2° Si u, d, c sont des nombres successifs, alors $A - A' = 198$.
3° Montrer que $A - A' = 99\,(c - u)$.

105. Soient deux nombres A et B. ($A > B$). On augmente A de 4 et on diminue en même temps B de 4. Comment sont modifiés la somme, la différence et le produit de ces deux nombres.

106. Soient les deux nombres A et B, tels que $A - B = 5$. On augmente ces deux nombres de 7, le produit augmente alors de 364. Calculer A et B.

107. Soit un nombre $A = \overline{cdu}$. Le nombre 3A est terminé par 638. Calculer A.

108. Calculer trois nombres entiers naturels a, b, c sachant que

$$\begin{cases} 2a = b + c \\ a + b + c = abc \end{cases}$$

109. La somme de p nombres successifs est un nombre donné A. Trouver ces p nombres.
Le problème est-il possible quel que soit A ? Donner les conditions de possibilité.

Exemples : $p = 3$ et $A = 165$
$p = 4$ et $A = 114$.

110. Quel est le plus grand nombre qui peut être ajouté au dividende d'une division sans changer le quotient ?

111. Quel est le plus grand nombre qui peut être ajouté au diviseur d'une division sans changer le quotient ?

112. Soit la division de A par B :

$$A = B \cdot 356 + 4623.$$

De combien peut-on augmenter à la fois A et B sans changer le quotient Q = 356.

113. Une suite récurrente est définie par

$$u_0 = 0 \qquad u_1 = 1 \qquad \text{et} \qquad u_{n+2} = u_{n+1} + u_n.$$

1° Donner les 20 premiers termes de cette suite.

2° Démontrer que

$$u_{n+2} = 1 + u_0 + u_1 + u_2 + \cdots + u_n.$$

3° Le carré d'un terme de cette suite, à partir de u_2, est égal au produit des termes qui l'encadrent augmenté ou diminué de 1; c'est-à-dire que :

$$(u_i)^2 = u_{i-1} \times u_{i+1} + 1$$

ou

$$(u_i)^2 = u_{i-1} \times u_{i+1} - 1$$

suivant la valeur de i.

114. On considère la suite récurrente :

$$u_1 = a \qquad u_2 = b \qquad \text{et} \qquad u_{n+2} = u_{n+1} + u_n.$$

On exclut de cette suite les termes qui ont le même nombre de chiffres que a ou b.

Démontrer qu'il y a 4 nombres au moins et 5 nombres au plus qui ont le même nombre de chiffres.

115. Démontrer :

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

116. Soit un tableau carré à n colonnes et n lignes (fig. Ex. 116). On numérote les lignes L_1, L_2, ... L_n et les colonnes C_1, C_2, ... C_n.

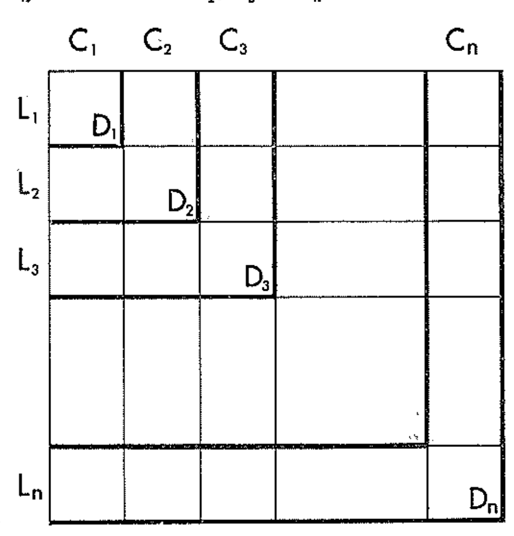


Fig. Ex. 116.

Soient :

$$D_1 = C_1 \cap L_1$$
$$D_2 = (C_1 \cup C_2) \cap (L_1 \cup L_2)$$
$$D^3 = (C_1 \cup C_2 \cup C_3) \cap (L_1 \cup L_2 \cup L_3)$$
....
$$D_n = (C_1 \cup \dots \cup C_n) \cap (L_1 \cup \dots \cup L_n).$$

A. On place 1 dans toutes les cases du tableau.

1° Démontrer que la somme des nombres placés dans $D_k - D_{k-1}$ est égale à $2k - 1$.

2° En conclure que la somme des n premiers nombres impairs est n^2.

B. Dans le tableau, on place :

dans la ligne L_1, les nombres $0;\ 1;\ 2;\ \dots;\ n-1;$
dans la ligne L_2, les nombres $1;\ 2;\ 3;\ \dots;\ n;$
dans la ligne L_3, les nombres $2;\ 3;\ 4;\ \dots;\ n+1;$
. . . .
dans la ligne L_n, les nombres $n-1;\ n;\ n+1;\ \dots;\ 2n-2$.

1° Montrer que la somme des nombres inscrits dans le tableau est $n^3 - n^2$.

2° Démontrer que la somme des nombres écrits dans $D_k - D_{k-1}$ est $3k^2 - 5k + 2$.

En conclure que la somme des nombres écrits dans le tableau est $3S_2 - 5S_2 + 2n$, S désignant la somme des n premiers nombres et S_2 la somme des carrés des n premiers nombres.

3° Montrer que :

$$S_2 = \frac{n(n+1)(2n+1)}{6}.$$

C. Dans le tableau on place :

dans la ligne L_1, les nombres $1;\ 2;\ 3;\ \dots;\ n;$
dans la ligne L_2, les nombres $2;\ 4;\ 6;\ \dots;\ 2n;$
dans la ligne L_3, les nombres $3;\ 6;\ 9;\ \dots;\ 3n;$
. . . .
dans la ligne L_n, les nombres $n;\ 2n;\ 3n;\ \dots;\ n^2$.

1° Montrer que la somme des nombres inscrits dans le tableau est n^2.

2° Démontrer que la somme des nombres écrits dans $D_k - D_{k-1}$ est k^3.

3° En déduire que la somme S_3 des cubes des n premiers nombres est $S_3 = n^2$.

117. Soit le nombre A = 324. Écrire ce nombre dans le système de base 5.

118. Un nombre est écrit dans le système de base $b = 5$: A = 324. Écrire ce nombre dans le système décimal.

119. Écrire le nombre 37 dans le système de base $b = 2$. (Système binaire).

120. Soit le nombre 1101101 dans le système binaire. Écrire ce nombre dans le système décimal.

Analyse combinatoire.

121. De combien de manières peut-on choisir un garçon et une fille parmi un groupe de 9 filles et 6 garçons ?

122. Calculer : $6!$ $\quad \frac{7!}{4!}$ $\quad \frac{8!}{5!\,3!}$

123. Exprimer en factorielles les nombres suivants :

$$10 \times 9 \times 8 \qquad 10 \times 11 \times 12 \times 13.$$

124. Exprimer en factorielles les nombres suivants :

$$n(n-1)(n-2) \qquad n(n+1)(n+2)(n+3).$$

125. De combien de façons peut-on choisir 3 livres dans un ensemble de 7 livres ?

126. De combien de façons peut-on former une équipe de football de 11 joueurs si on dispose de 14 joueurs ?

127. De combien de façons peut-on choisir 3 cartes dans un jeu de 52 cartes ?

128. Quel est le plus grand nombre de points d'intersection de 12 droites distinctes de 9 cercles distincts; de 6 droites distinctes et 5 cercles distincts ?

129. De combien de manières peut-on former un groupe de 4 hommes et 3 femmes lorsqu'il y a 10 hommes et 8 femmes ?

130. J'ai écrit 10 lettres mais je ne dispose que de 4 timbres. De combien de manières puis-je choisir les lettres à timbrer ?

131. De combien de façons peut-on séparer un groupe de 10 élèves en deux groupes de 3 et 7 élèves respectivement ?

132. Dans un groupe de 15 garçons, il y a 7 boy-scouts. De combien de façons peut-on choisir 12 garçons de sorte qu'il y ait 6 boy-scouts ? Même problème de sorte qu'il y ait au moins 4 boy-scouts.

133. Un comité de 6 personnes doit être choisi parmi 10 hommes et 7 femmes de sorte qu'il contienne au moins 3 hommes et deux femmes. Deux des femmes refusent d'entrer dans ce comité. De combien de façons peut-on former ce comité ?

134. Simplifier : $C_n^n \times C_{3n}^{2n} \times C_{2n}^n$.

135. Simplifier : $C_{n+1}^3 : C_n^2$ et $C_{n+1}^{r+1} : C_n^r$.

136. Déterminer n pour que :

$$C_n^3 = C_n^5 \qquad \text{et} \qquad C_n^2 = 55.$$

137. Combien y a-t-il de diagonales dans un polygone de n côtés.

138. On marque n points sur un cercle. Combien obtient-on de cordes en joignant les points deux à deux ?

139. Exprimer en factorielles

$$A = n(n^2-1)(n^2-4)(n^2-9)$$
$$B = n(n+1)(n+2)(n+3)\ \dots\ (n+r).$$

140. Simplifier :

$$\frac{n!}{(n-1)!} \qquad n! - (n-1)!$$

141. Prouver que

$$\frac{(2n)!}{n!} = 2^n \cdot [1 \times 3 \times 5 \times 7 \times \cdots \times (2n-1)].$$

142. A-t-on :

$$2 \times 6 \times 10 \times 14 \times \dots \times (4n-6)(4n-2) = (n+1)(n+2)(n+3) \dots (2n-1) \cdot 2n\ ?$$

143. Prouver que

$$(2n+1)(2n+3)(2n+5) \cdots (4n-3)(4n-1) = \frac{(4n)!\, n!}{2_n\,[(2n)!]^2}.$$

144. Calculer n sachant que $A_n^3 = 240\,n$.

145. Calculer m sachant que $C_{2m}^1 + C_{2m}^2 + C_{2m}^3 = 387$ m.

146. Calculer x et y sachant que

$$\begin{cases} C_x^y = C_x^{y+1} \\ 4\,C_x^y = 5\,C_x^{y-1}. \end{cases}$$

147. Calculer x sachant que

$$C_x^{a+b} = C_x^{a-b}.$$

148. Démontrer les formules

1° $$k\,C_n^k = n\,C_{n-1}^{k-2}$$

2° $$C_{n+2}^{r+1} = C_n^{r+1} + C_n^{r-1} + 2\,C_n^r.$$

149. Démontrer :

1° $$C_m^k \cdot C_{m-k}^{p-k} = C_m^p \cdot C_p^k \qquad (m > p > k)$$

2° $$C_n^p = \left(\frac{n+1}{p}\right) \cdot C_m^{p-1}$$

Anneau Z. Congruences dans Z.

150. Déterminer x pour que $\overline{247\,x}$ soit divisible par 2.

151. Déterminer x pour que $\overline{148\,x}$ soit divisible par 4.

152. Déterminer x et y pour que $\overline{4x\,5y}$ soit divisible par 6.

153. Déterminer x pour que $\overline{231\ x}$ soit divisible par 3.

154. Déterminer x pour que $\overline{2\,x\,4\,5}$ soit divisible par 9.

155. Déterminer x et y pour que $\overline{4\,x\,3\,y}$ soit divisible par 2 et par 9.

156. Déterminer x et y pour que $\overline{5\,x\,4\,y}$ soit divisible par 11.

157. Déterminer le nombre $A = \overline{du}$ tel que $\overline{du} = 3d \cdot u$.

158. Démontrer :

$$(\forall n) \qquad 2 \mid n\,(n+1).$$

159. Déterminer les nombres A et B sachant que

$$2A = B\,(A - B)$$

ou

$$2B = A\,(A - B).$$

160. Démontrer :

$$a^{n+4} - a^n = 0, \text{ mod. } 10.$$

161. Soit $X = \overline{cdu}$. On sait que

$$c + d + u = 13$$
$$u = 3c$$
$$\overline{cdu} + 396 = \overline{udc}.$$

Calculer le nombre X.

162. Le nombre 481 635 est-il divisible par $495 = 5 \times 9 \times 11$, et pourquoi ?

163. Calculer le reste de la division de 314 532 par 11 sans faire la division.

164. Quel est le reste de la division de $(57383)^4$ par 19 ?

165. Montrer que 29 461 905 est divisible par 495, sans faire la division.

166. Résoudre dans N

$$(x - 6)(y - 6) = 18.$$

167. Résoudre dans N :

$$x^2 = (y - 7)^2 + 21.$$

168. Soit le nombre $A = \overline{mcdu}$.

Démontrer que le nombre

$$\overline{mcdu} + \overline{udcm}$$

est divisible par 11.

169. Démontrer les implications :

1° $[A + 1 = 0, \text{ mod } p] \Rightarrow [A^{2n} - 1 = 0, \text{ mod } p]$

2° $[A + 1 = 0, \text{ mod } p] \Rightarrow [A^{2n+1} + 1 = 0, \text{ mod } p]$.

170. Si le nombre n n'est pas multiple de 3, démontrer que

$$2^{2n} + 2^n + 1 = 0, \text{ mod. } 7.$$

171. n n'étant pas multiple de 3, on a :

$$3^{2n} + 3^n + 1 = 0, \text{ mod. } 13.$$

172. n n'étant pas multiple de 3, on a :

$$5^{2n} + 5^n + 1 = 0, \text{ mod } 31.$$

173. Démontrer :

$$(\forall n) : \quad 3^{2n+2} + 2^{6n+1} = 0, \text{ mod. } 11.$$

174. Démontrer :

$$(\forall n) \quad 3^{2n+2} - 2^{n+1} = 0, \text{ mod } 7.$$

175. Démontrer :

$$(\forall n) \quad 3^{2n+3} + 2^{n+3} = 0, \text{ mod } 7.$$

176. Démontrer :

$$(\forall n) \quad 3 \cdot 5^{2n+1} + 2^{3n+1} = 0, \text{ mod } 17.$$

177. Calculer x sachant que

$$(2601)^{187} = x, \text{ mod } 11.$$

178. Calculer x sachant que

$$(82324)^{625} = x, \text{ mod } 7.$$

179. Soit le nombre $A = 3012^{93} \times 163034^{39} \times 4^{67}$.
Calculer x tel que

$$A = x, \text{ mod } 43.$$

180. Calculer x, y... :

$$10 = x, \quad \text{mod } 7$$
$$10^2 = y, \quad \text{mod } 7$$
$$\dots\dots\dots\dots$$
$$10^n = z, \quad \text{mod } 7.$$

Trouver un critère de divisibilité par 7.

181. Trouver des critères de divisibilité par 13, par 19, par 21, par 37.

182. Soient $x \in N$ et $y \in N$.
Les deux assertions :

a) x et y sont divisibles par 7;
b) $x^2 + y^2$ est divisible par 7;

sont équivalentes.

183. Démontrer l'équivalence :

$$[11 \mid x \quad \text{et} \quad 11 \mid y] \Leftrightarrow [11 \mid x^2 + y^2].$$

184. Calculer x tel que

$$10^{6n+2} + 10^{3n+1} + 1 = x, \text{ mod } 7.$$

Nombres premiers. P.G.C.D. P.P.C.M.

185. Décomposer les nombres suivants en facteurs primaires :

21 879; 111 111; 15 015.

186. Calculer le P.G.C.D. de A et B :

1° A = 63 083 et B = 35 455.
2° A = 3 570 et B = 4 515.

187. Calculer le P.P.C.M. de A = 9 827 et B = 6 974.

188. Déterminer les diviseurs communs des nombres 364 et 476; des nombres 18 459 et 3 809 ?

189. Trouver l'ensemble des diviseurs de 540.

190. Les nombres suivants sont-ils premiers : 1 409; 1 009 ?

191. Trouver deux nombres connaissant leur P.G.C.D. 6 et leur produit 2 700.

192. a étant un nombre entier naturel quelconque, on considère les nombres

$$A = 35a + 57 \quad \text{et} \quad B = 45a + 76.$$

Montrer que $A \wedge B$ est égal à 19 ou à 1.

193. a et b étant des nombres entiers quelconques, on envisage les nombres $A = 11a + 2b$ et $B = 18a + 5b$.

1° Démontrer l'équivalence

$$19 \mid A \Leftrightarrow 19 \mid B$$

2° On suppose $a \wedge b = 1$, montrer que A et B ne peuvent avoir d'autre diviseur commun que 19 et 1.

194. Démontrer :

$$(\forall a)(\forall b) \qquad a \wedge b = (5a + 3b) \wedge 13a + 8b).$$

195. Sachant que $mn' - nm' = 1$, démontrer :

$$(\forall a)(\forall b) \qquad a \wedge b = (ma + nb) \wedge (m'a + n'b).$$

196. Résoudre dans N :

$$\begin{cases} x + y = 84 \\ x \wedge y = 12 \end{cases}$$

197. Sachant que

$$4373 = 8, \text{ mod } p$$

et

$$826 = 7, \text{ mod } p,$$

calculer p.

198. Démontrer l'implication suivante :

$$\left.\begin{array}{l} a' \wedge c = 1 \\ \text{et} \\ c \mid ab - a'b' \\ \text{et} \\ c \mid a - a' \end{array}\right\} \Rightarrow c \mid b - b'.$$

199. Démontrer que, quel que soit n, $n(n+2)(5n-1)(5n+1)$ est divisible par 24.

200. Démontrer :

$(\forall n)$; $\qquad 12 \mid n^2(n^2-1)$.

201. Démontrer :

$(\forall n)$: $\qquad 60 \mid n^2(n^4-1)$.

202. Démontrer :

$(\forall n)$: $\qquad 6 \mid n(n+1)(7n+2)$.

203. Démontrer :

$(\forall a)(\forall b)$: $\qquad 30 \mid ab(a^2+b^2)(a^2-b^2)$.

204. Démontrer l'implication :

$$m \wedge a = 1 \quad \Rightarrow \quad ma \wedge c = a \wedge c.$$

205. Démontrer la formule :

$$A^n \wedge B^n = (A \wedge B)^n.$$

206. Résoudre dans N :

$$x \vee y = 51\,840$$
$$x \wedge y = 2160.$$

207. Déterminer l'ensemble des diviseurs de 900.
En déduire la résolution dans N de l'équation

$$(x-3)(y-4) = 900.$$

208. Résoudre dans N :

$$2xy + 2x + y = 99.$$

209. Quel est le plus petit nombre qui, divisé par 3195 et par 477 donne 9 pour reste ?

210. Calculer :

$$(6 \times 345\,695) \wedge (15 \times 345\,695)$$

et

$$(6 \times 345\,695) \vee (15 \times 345\,695)$$

211. Calculer x sachant que $12 \vee x = 60$.

212. n étant un entier quelconque, calculer $n \vee (n+1) \vee (n+2)$.

213. 1° Démontrer l'implication :

$$[a \wedge b = 1] \quad \Rightarrow \quad [(a+b) \wedge ab = 1].$$

2° Démontrer :

$(\forall n)$ $\qquad (2n+1) \wedge 2n(n+1) = 1$.

214. Démontrer l'implication :

$$[a \vee b \vee c = abc] \quad \Rightarrow \quad [a \wedge b = 1 \text{ et } a \wedge c = 1 \text{ et } b \wedge c = 1].$$

215. Quel est le plus petit nombre qui admet 15 diviseurs.

216. Démontrer l'implication :

$$\left.\begin{array}{l} a \wedge b = 1 \\ \text{et} \\ m \wedge a = 1 \\ \text{et} \\ m \wedge b = 1 \end{array}\right\} \quad \Rightarrow \quad m \wedge ab = (m \wedge a) \cdot (m \wedge b).$$

217. Démontrer les implications :

1° $a \wedge b = 1 \Rightarrow ab \wedge (a + b) = 1.$

2° $a \wedge b = 1 \Rightarrow (a + b) \wedge (a^2 + b^2) = 1.$

218. a, b, c, d étant des entiers naturels quelconques, on a :

$$(ab \wedge c)\,(a \wedge cd) \mid (ab \wedge cd)\,(a \wedge c).$$

219. 1° Démontrer la formule :

$$a \wedge b = (a + b) \wedge (a \vee b).$$

2° Résoudre dans N :

$$x + y = 69\,384$$
$$x \vee y = 2\,450\,448$$

220. Démontrer la formule :

$$a \vee b \vee c = (a \vee b) \vee (a \vee c).$$

221. Calculer en fonction de $\Delta = a \wedge b$ et de $\mu = a \vee b$, les nombres

$$A = a^2 \wedge ab \wedge b^2$$

et

$$B = a^2 \vee ab \vee b^2.$$

222. Si a est un nombre impair, $a^3 - a$ est divisible par 24.

223. Si le nombre premier p ne divise pas a, il divise $a^{p-1} - 1$. (Théorème de Fermat.)

224. a et p étant premiers entre eux, on a :

$$a \times 2a \times 3a \times \ldots \times (p-1)\,a = 1 \times 2 \times 3 \times \ldots \times (p-1), \text{ mod } p$$

225. 1° Quel est le P.G.C.D. de 14 865 et 7 976.

2° Un terrain a la forme d'un triangle dont les côtés ont pour mesures 132 m; 156 m et 204 m. On veut planter des arbres sur son périmètre de façon à ce qu'il y ait un arbre à chaque sommet du triangle et que les arbres soient également espacés. Quel est le nombre minimum d'arbres que l'on pourra planter, si l'on veut que la distance entre deux arbres puisse s'exprimer par un nombre entier de mètres.

Corps Q des rationnels.

226. Trouver les fractions équivalentes à la fraction $\frac{114}{226}$ dont le numérateur est inférieur à 400 et le dénominateur supérieur à 600.

227. Une fraction est équivalente à $\frac{117}{260}$. Trouver les deux termes de cette fraction sachant que leur P.G.C.D. est 36. Quel est alors leur P.P.C.M.

228. La fraction $\frac{a + 17}{a - 4}$ peut-elle se réduire à un nombre entier?

229. Trouver une fraction équivalente à $\frac{105}{375}$ sachant que ses termes ont pour P.G.C.D. 31.

230. Soit une fraction $\frac{a}{b}$; quels nombres x et y peut-on ajouter respectivement au numérateur et au dénominateur pour obtenir une fraction équivalente à la fraction $\frac{a}{b}$?

231. Montrer que si $ab' - ba' = 1$, les fractions $\frac{a}{b}$; $\frac{a'}{b'}$; $\frac{a+a'}{a}$; $\frac{a+a'}{b+b'}$ sont irréductibles.

232. Déterminer les fractions $\frac{x}{y}$ telles que les fractions $\frac{x-27}{y}$ et $\frac{x}{y+12}$ soient équivalentes.

233. Calculer :

$$\frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \cdots + \frac{1}{n(n+1)}.$$

234. Calculer :

$$\frac{1}{1 \times 3} + \frac{1}{3 \times 5} + \cdots + \frac{1}{(2n+1)(2n+3)}.$$

235. n étant un nombre entier :

1° Pour quelles valeurs de n, la fraction $\frac{n+8}{2n-5}$ représente-t-elle un nombre entier ?

2° Pour quelles valeurs de n cette fraction est-elle irréductible ?

3° Si la fraction n'est pas irréductible, quels peuvent être les diviseurs communs du numérateur et du dénominateur ?

236. 1° Démontrer que

$$\frac{a}{b} + \frac{b}{a} \geqslant 2.$$

2° Déterminer la fraction $\frac{a}{b}$ telle que

$$\frac{a}{b} + \frac{b}{a} - 2 = \frac{9}{70}.$$

237. Démontrer :

$$\left(\forall \frac{a}{b}\right), \quad \frac{a}{b} \in \mathrm{Q}, \quad (\exists n) \ n \in \mathrm{N} : \quad \left|\frac{a}{b} - n\right| \leqslant \frac{1}{2}.$$

238. Tout nombre rationnel A peut s'écrire de façon unique sous la forme :

$$\mathrm{A} = \frac{\alpha_1}{1!} + \frac{\alpha_2}{2!} + \frac{\alpha_3}{3!} + \cdots + \frac{\alpha_n}{n!}$$

avec :

$$\begin{gathered} \alpha_1 \in \mathrm{Z} \\ |\alpha_2| < 2 \\ |\alpha_3| < 3 \\ \cdots\cdots \\ |\alpha_n| < n. \end{gathered}$$

Application numérique : $\mathrm{A} = \frac{142}{30}$.

239. Résoudre dans N :

$$\left\{ \begin{array}{l} \frac{x}{y} - \frac{u}{v} = \frac{5}{6} \\ x \wedge u = x - u \\ x \vee u = 1\,050 \end{array} \right.$$

240. Quel est le plus grand des deux nombres :

$$A = 5 + \frac{7}{9} + \frac{8}{9^2} + \frac{6}{9^3} + \frac{8}{9^4}$$

et

$$B = 5 + \frac{7}{9} + \frac{8}{9^2} + \frac{7}{9^3} + \frac{1}{9^4}.$$

241. Trouver une fraction $\frac{a}{b}$ sachant qu'elle est équivalente à 0,375 et que le produit de ses deux termes est 384.

242. Résoudre dans N :

$$x \wedge y = 1$$
$$\frac{x + y}{x^2 - xy + y^2} = \frac{10}{37}.$$

243. Quel que soit le nombre entier n, les fractions

$$\frac{n-1}{n}; \quad \frac{n}{2n+1}; \quad \frac{2n+1}{2n^2+2n}$$

sont irréductibles.

244. Les fractions $\frac{1\,023}{2\,750}$ et $\frac{1\,243}{3\,750}$ sont-elles décimales ?

245. Quelles sont les fractions décimales équivalentes à $\frac{39}{78}$; à $\frac{182}{130}$?

246. La somme de deux fractions décimales est une fraction décimale. La réciproque est-elle vraie?

247. La fraction $\frac{693}{17\,325}$ est-elle décimale ?

Corps R des réels.

248. Calculer $\sqrt[8]{5}$ à $\frac{1}{10^2}$ près.

249. On considère le nombre

$$\sqrt{n^2 + \sqrt{4n^2 + \sqrt{16n^2 + 8n + 3}}}, \qquad n \in N$$

Montrer que $n + 1$ et $n + 2$ constituent un encadrement de A.

250. Calculer $\pi\sqrt{5}$ à 0,001 près.

251. Calculer $\frac{\sqrt{5}}{\sqrt{3}}$ à 0,001 près.

252. Calculer $\sqrt{\frac{2\pi}{\sqrt{5}}}$ à 0,01 près.

253. Calculer $\sqrt{\frac{4 - \sqrt{15}}{4 + \sqrt{15}}}$ à 0,01 près.

254. Soient les nombres :

a = 0,235 ... à 0,001 près;
b = 1,032 ... à 0,001 près.

Calculer l'erreur absolue commise sur $ab + b^2$.

255. Soient les nombres :

$$a = 1{,}732 \ldots \text{ à } 0{,}01 \text{ près;}$$
$$b = 4{,}030 \ldots \text{ à } 0{,}001 \text{ près.}$$

Calculer l'erreur absolue commise sur $ab + a$.

256. Soient les nombres :

$$a = 2{,}032 \ldots \text{ à } 0{,}001 \text{ près;}$$
$$b = 3{,}041 \ldots \text{ à } 0{,}001 \text{ près;}$$
$$c = 0{,}141 \ldots \text{ à } 0{,}001 \text{ près.}$$

Calculer l'erreur absolue et l'erreur relative commises sur $\frac{ab}{c}$.

257. Quelles sont les fractions de la forme $\frac{7}{x}$ dont la valeur approchée par défaut à $\frac{1}{10^3}$ près est 0,636.

258. Soit la fraction $\frac{n+13}{n-2}$.

Pour quelles valeurs de n est-elle équivalente à un nombre entier ?
Pour quelles valeurs de n est-elle irréductible ?
Sa valeur approchée par défaut à 0,1 près est-elle-1,8 ?

259. Trouver la fraction qui engendre le développement décimal 3,278 181 818 ...

260. Trouver la fraction de développement décimal périodique 3,212 121 ...

261. Trouver le développement décimal de $\frac{3}{7}$; de $\frac{5}{6}$; de $\frac{7}{30}$.

262. Quelles sont les fractions génératrices des nombres périodiques suivants :

1° 0,454 545 ...
2° 0,312 312 ...
3° 0,215 151 ...
4° 1,224 242 ...

263. Montrer que, quel que soit n, le nombre rationnel

$$A = \frac{1}{n} + \frac{1}{n+1} + \frac{1}{n+2},$$

a un développement décimal illimité périodique mixte.

Corps C des complexes.

264. Soient les nombres z et z'. Calculer z + z' et z — z'.

1° $z = 1 - 4i$ $z' = 6 + 2i$
2° $z = 5 + 8i$ $z' = 8 + 5i$
3° $z = -6 + 9i$ $z' = 1 - i$
4° $z = 7 + 8i$ $z' = -3 + 5i$

265. Effectuer les opérations suivantes :

1° $(1 + i) + (-1 + 3i) + (3 - 4i)$
2° $(3 - 2i) + (2 + 4i) + (-1 + 5i)$
3° $(2 + i) - (3 - i) + (1 + 3i)$
4° $(2 - 3i) - (-1 - i) - 3 + 3i)$.

266. Effectuer les opérations suivantes :

1° $3\ (2 - 5\,i)$

2° $-2\,i\,(2 + i\ )$

3° $(2 + 3\,i)\quad(3 + 2\,i)$

4° $(3 - i\sqrt{5})(4 - 2\,i\sqrt{5})$

267. On donne z et z'. Calculer zz'.

1° $z = -7 + i \qquad z' = 7 + i$

2° $z = \sqrt{3} - i\sqrt{5} \qquad z' = \sqrt{3} + i\sqrt{5}$

3° $z = -2 + 7\,i \qquad z' = -2 - 7\,i$

4° $z = x - a + bi \qquad z' = x - a - bi$

268. Calculer les produits suivants :

1° $(2 + i)\,(1 + 2\,i)$

2° $(1 + i)\,(2 - 5\,i)$

3° $(1 - i)\,(2 + 2\,i)$

4° $-(3 - i\ )\quad(2 + 3\,i)$

5° $(-1 + 3\,i)\,(3 - 5\,i)$

6° $(-2 - 2\,i)\,(-1 + 3\,i)$

269. Soient les complexes z et z'. Calculer $\frac{z}{z'}$.

1° $z = 1 + i \qquad z' = 2 + i$

2° $z = 3 \qquad z' = 6 - 5i$

3° $z = 9 - i \qquad z' = i$

4° $z = a + ib \qquad z' = b - ai$

270. Effectuer les opérations suivantes :

1° $$\frac{a + bm - (am - b)\,i}{1 - mi}$$

2° $$\frac{a + bi}{a - bi} + \frac{a - bi}{a + bi}.$$

271. 1° Calculer :

$$(a + ib)\,(a - ib)$$

2° Calculer :

$$(a + ib)\,(c + id)$$

3° Transformer $(a^2 + b^2)\,(c^2 + d^2)$ en une somme de deux carrés.

4° Transformer en une somme de deux carrés :

a) 5×29

b) $5 \times 13 \times 29$

c) $(a^2 + b^2)^2$

272. Transformer en une somme de deux carrés :

1° $(a^2 + b^2)^3$

2° $(a^2 + b^2)\,(a'^2 + b'^2)\,(a''^2 + b''^2)$

3° $(a^2 + b^2)^2\,(c^2 + d^2)^2$

273. Rechercher les racines carrées des nombres Z suivants :

1° $Z = 3 + 4\,i$

2° $Z = -3 - 4\,i$

3° $Z = 15 - 20\,i$

4° $Z = -6 + 8\,i$

5° $Z = 7 + 6\,i\sqrt{2}$

6° $Z = 2 - 4\,i\sqrt{6}$

(on posera $Z = z^2$ et $z = x + iy$)

274. Mettre sous forme analytique les nombres

$$\frac{2-i}{3+2i}; \qquad (1+i)^7; \qquad \left(\frac{\sqrt{3}-i}{1+i\sqrt{3}}\right)^9$$

275. Décomposer en facteurs du 2e degré :

$$A = (x^2 + y^2 - 1) + 4x^2$$

276. Soit le nombre $z = x + iy$. On considère le nombre complexe $Z = \frac{z-1}{z+1}$. Calculer $\mathcal{R}e\,(Z)$ et $\mathcal{I}m\,(Z)$. Évaluer $|Z|$.

277. Calculer :

1° $(2 - i\sqrt{3})^2 - (2 + i\sqrt{3})^2$

2° $(2 - i\sqrt{3})^3 - (2 + i\sqrt{3})^3$.

278. Soit le nombre complexe $j = \frac{-1 + i\sqrt{3}}{2}$. Calculer j^2 et j^3.

279. Soit le nombre complexe $j = \frac{-1 + i\sqrt{3}}{2}$. Calculer $1 + j + j^2$.

280. z étant un nombre complexe quelconque, $z = x + iy$, on considère le nombre

$$Z = \frac{z^2}{z+i}.$$

Calculer, en fonction de x et de y, $\mathcal{R}e\,(Z)$ et $\mathcal{I}m\,(Z)$.

281. Soit $z = x + iy$. Montrer que

$$|z|\sqrt{2} \geqslant |x| + |y|.$$

282. Soit $z = x + iy$. Calculer $z\bar{z} - z^2$ et $\bar{z}^2 - z\bar{z}$.

283. Soit $z + \frac{1+ix}{1-ix}$ avec $x \in \mathbb{R}$. Calculer $|z|$.

Suites finies. Progressions.

284. Développer :

$$\sum_{i=1}^{i=n} i\,(i+1) \qquad \sum_{n}^{i=2n} (i\,!) \qquad \sum_{\alpha=0}^{\alpha=n-1} (\alpha+1)\,\alpha^{\alpha}$$

$$\sum_{1}^{n} r \qquad \sum_{n}^{2n} (2r-1) \qquad \sum_{1}^{n} r\,(r-1).$$

285. Utiliser le symbole Σ pour exprimer les sommes :

1° $1 \times 3 + 2 \times 4 + 3 \times 5 + 4 \times 6 + \cdots$ (n termes)

2° $1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots$ (n termes)

3° $\frac{1}{n^2} + \frac{1}{(n+1)^2} + \frac{1}{(n+2)^2} + \cdots + \frac{1}{(2n)^2}$.

286. Sachant que :

$$\sum_{1}^{n} r^3 = \frac{n^2 (n + 1)^2}{4},$$

calculer :

$$\sum_{n}^{2n} r^2.$$

287. 1° Montrer que

$$\sum_{1}^{n} r (a + 1) = \frac{n (n + 1) (n + 2)}{3}$$

2° Calculer :

$$\sum_{1}^{n} r (x - 1) \qquad \text{et} \qquad \sum_{1}^{n+1} r (r + 1).$$

288. On donne $f(x) = \frac{1}{x}\cdot$

1° Montrer que

$$f(x) - f(x + 1) = \frac{1}{x (x + 1)}$$

2° En déduire la valeur de $\sum_{1}^{n} \frac{1}{x (x + 1)}\cdot$

289. Montrer que :

$$\frac{1}{n (n + 1)} = \frac{1}{n} - \frac{1}{n + 1}$$

En déduire la somme :

$$\frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \frac{1}{3 \times 4} + \cdots + \frac{1}{n (n + 1)}\cdot$$

290. Montrer que :

$$(2 x + 1)^3 - (2 x - 1)^3 = 24 x^2 + 2$$

En déduire la somme :

$$1^2 + 2^2 + 3^2 + \ldots + n^2$$

291. Montrer que :

$$4 x^3 = f(x + 1) - f(x)$$

avec :

$$f(x) = [(x - 1) x]^2$$

292. En déduire :

$$\sum_{x=1}^{n} x^3$$

293. Montrer que :

$$r (r + 1) (r + 2) - (r - 1) r (r + 1) = 3 r (r + 1)$$

En déduire la somme :

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots + n (n + 1)$$

294. Montrer que :

$$r(r+1)(r+2)(r+3) - (r-1)r(r+1)(r+2) = 4r(r+1)(r+2)$$

En déduire :

$$\sum_1^n r(r+1)(r+2) = \frac{n(n+1)(n+2)(n+3)}{4}.$$

295. Calculer :

1° $$\sum_1^n r(r+3)$$

2° $$\sum_1^n r(r+3)(r+6).$$

296. Calculer :

1° $$\sum_1^n p(p^2-1)$$

2° $$\sum_1^n (p+1)^3.$$

297. Calculer :

1° $$\sum_1^n p(p+1)(2p+1)$$

2° $$\sum_1^n p(p+1)(p+3)(p+4).$$

298. Montrer que :

1° $$\sum_1^n \frac{1}{4r^2-1} = \frac{n}{n+1}$$

2° $$\sum_1^n \frac{1}{(3r-2)(3r+1)} = \frac{n}{3n+1}.$$

299. Montrer que :

1° $$\sum_1^n p \cdot p! = (n+1)! - 1$$

2° $$\sum_1^n (p^2+1) \cdot p! = n \cdot (n+1)!$$

300. Soit la suite récurrente

$$u_{n+1} = 2u_n + 1.$$

Prouver que :

$$u_n + 1 = 2^{n-1} \cdot (u_1 + 1)$$

Calculer :

$$\sum_1^n u_p \quad \text{avec} \quad u_1 = 1.$$

301. Une progression arithmétique commence par $u_1 = 2i$ et sa raison est $r = 2$. Calculer le terme u_n et la somme $S_n = u_1 + u_2 + ... + u_n$.

302. Une progression arithmétique de 100 termes a pour premier terme $u_1 = -1 + i$ et la raison est $r = 1 + i$. Calculer le dernier terme et la somme des termes de cette progression.

303. Une progression arithmétique de 100 termes a pour somme — 16 350, et pour dernier terme — 312.
Calculer le premier terme et la raison.

304. Une progression arithmétique a pour premier terme 175 et pour dernier terme — 225. Sa somme est — 2 025.
Calculer la raison de cette progression et le nombre de termes.

305. Montrer que les nombres :

$$a = (x^2 - 2x - 1)^2$$
$$b = (x^2 + 1)^2$$
$$c = (x^2 + 2x - 1)^2$$

sont en progression arithmétique.

306. a, b, c étant trois nombres en progression arithmétique, démontrer que l'on a :

$$2(a^3 + b^3 + c^3) + 21\,abc = 3(a + b + c)(ab + bc + ca).$$

La réciproque est-elle vraie ?

307. Une progression géométrique a pour premier terme $u_1 = i$ et pour raison $q = \frac{1}{2}$. Calculer le dixième terme et la somme de ces 10 termes.

308. La somme des termes d'une progression géométrique est $S = 17\,089\,842$. Le premier terme est $u_1 = 7$; le nombre de termes est $n = 10$. Calculer la raison et le dernier terme.

309. Calculer trois nombres x, y, z en progression géométrique sachant que

$$x + y + z = a$$

et

$$x^2 + y^2 + z^2 = b^2$$

310. On considère une progression arithmétique de 4 termes :

$$u_1 \quad u_2 \quad u_3 \quad u_4$$

A ces termes on ajoute respectivement :

$$3 \quad 5 \quad 9 \quad 21$$

et on obtient alors les 4 termes consécutifs d'une progression géométrique.
Trouver les 4 termes u_1, u_2, u_3, u_4 de la progression arithmétique donnée.

Problèmes.

311. 1° p étant un entier positif et n un entier positif plus grand que *un*, on considère les nombres

$$a = p \cdot n, \qquad b = p \cdot (n - 1)$$

Démontrer que le plus grand commun diviseur de ces deux nombres est égal à leur différence. Inversement, démontrer que si deux nombres entiers positifs a et b admettent leur différence comme plus grand commun diviseur, ils sont de la forme

$$a = p \cdot n, \qquad b = p(n - 1)$$

p et n désignant des entiers.

2° Déterminer deux entiers positifs admettant leur différence comme plus grand diviseur, sachant que leur plus petit commun multiple est 30. (Le problème admet plusieurs solutions.)

3° x et y étant deux entiers positifs donnés, on considère les trois nombres

$$A = 24x(5y+3) \qquad B = 15x(8y+5) \qquad C = 40x(3y+2)$$

Démontrer que le plus grand commun diviseur de deux quelconques d'entre eux est égal à leur différence. Calculer, en fonction de x et de y, le plus grand commun diviseur des trois nombres.

312. Soit une progression arithmétique dont le premier terme est 1 et la raison x.

1° Quelle doit être la raison pour que la somme des 100 premiers termes soit égale à 1 ? Y a-t-il un terme nul et dans ce cas quel est son rang ?

2° On forme le produit des trois premiers termes; déterminer la raison de manière que le rapport de ce produit au quatrième terme soit au nombre donné p. Discussion : existence et signe des racines de l'équation trouvée.

313. Dans ce qui suit on représente par des lettres minuscules des entiers rationnels, c'est-à-dire des éléments de Z. On représente par des lettres majuscules tout nombre de la forme $N = a + b\sqrt{2}$ avec $a \in Z$ et $b \in Z$.

1° Démontrer que si N est nul, a et b sont nuls. Démontrer plus généralement que si le nombre $N = a + b\sqrt{2}$ est égal au nombre $N_1 = a_1 + b_1\sqrt{2}$, on a $a = a_1$ et $b = b_1$.

Si on désigne par E l'ensemble des nombres de la forme $N = a + b\sqrt{2}$, montrer que la multiplication est loi interne dans E.

2° On suppose $|a|$ et $|b|$ non nuls et premiers entre eux pour le nombre $N = a + b\sqrt{2}$. On suppose en outre qu'il existe un nombre $N_1 = a_1 + b_1\sqrt{2}$ tel que le produit $N \cdot N_1$ soit un entier relatif. Montrer que a_1 et b_1 sont de la forme

$$a_1 = ka, \qquad b_1 = -kb,$$

$k \in Z$.

On suppose maintenant $N \cdot N_1 = 1$ et $|b| \neq 0$. Montrer qu'il en résulte $|a| \neq 0$ et $|a|$ et $|b|$ premiers entre eux.

$N = a + b\sqrt{2}$ étant donné, montrer que la condition nécessaire et suffisante pour qu'il existe N_1 tel que $N \cdot N_1 = 1$ est que $a^2 - 2b^2 = \pm 1$.

Donner l'expression du nombre N_1, inverse de N.

3° On appelle *nombre unitaire* tout nombre $N = a + b\sqrt{2}$ qui vérifie la condition $a^2 - 2b^2 = \pm 1$. Vérifier que le produit et le quotient de deux nombres unitaires sont encore des nombres unitaires. Vérifier que $1 + \sqrt{2}$ est un nombre unitaire.

4° Soit $N = a + b\sqrt{2}$ un nombre unitaire dans lequel on suppose a et b positifs. En comparant les carrés des nombres b, a, $2b$, démontrer la double inégalité $b \leqslant a < 2b$.

Former le quotient $N_1 = a_1 + b_1\sqrt{2}$ du nombre N par le nombre $1 + \sqrt{2}$.

Montrer que $N_1 = 1$ lorsque $a = b$ et que, dans l'hypothèse $a \neq b$, les nombres a_1 et b_1 vérifient :

$$0 < a_1 < a, \qquad 0 < b_1 < b.$$

En conclure que les divisions successives par $1 + \sqrt{2}$ aboutissent au nombre 1 après un nombre fini d'opérations, et qu'il existe un entier positif n tel que $N = (1 + \sqrt{2})^n$.

Montrer que tous les nombres unitaires sont donnés par la formule

$$N = \pm (1 + \sqrt{2})^r, \quad \text{où } r \in Z.$$

314. 1° On considère la progression géométrique

$$1, \ 3, \ 9, \ 27, \ 81, \ \dots$$

Quelle est le terme de rang? Montrer que les différences entre deux termes successifs forment une progression géométrique. Cette propriété peut-elle être généralisée?

2° Calculer la somme de la progression géométrique :

$$A_n = x + x^2 + \dots + x^n$$

En déduire la somme :

$$A'_n = 1 + 2x + 3x^2 \dots + nx^{n-1}.$$

Quelle forme prennent les expressions trouvées pour A_n et A'_n lorsqu'on y fait $x = 1$? Quelles sont en réalité les valeurs de A_n et A'_n pour $x = 1$?

3° Obtenir également des expressions des sommes suivantes :

$$1 + 3x^2 + 5x^4 + \dots + (2n + 1)x^{2n},$$
$$1 + 4x + 9x^2 + 16x^3 + \dots + n^2x^{n-1}.$$

315. On considère deux nombres entiers positifs a et b ($a > b$) et l'on désigne par d leur plus grand commun diviseur, par M leur plus petit commun multiple.

1° n étant un nombre entier naturel, chercher d et M, quand

$$a = n(2n - 1), \qquad b = (n - 1)2n - 1)$$

et justifier les résultats.

2° Exprimer les nombres a et b tels que

$$M \cdot (a + b) = a \cdot b \cdot d. \qquad (1)$$

en fonction de

$$p = \frac{a}{d} \quad \text{et} \quad q = \frac{b}{d}\cdot$$

3° Parmi les entiers qui vérifient la relation (1) trouver ceux qui satisfont à

$$d = a - b. \qquad (2)$$

4° Montrer que les nombres entiers a et b qui vérifient simultanément (1) et (2) vérifient

$$(a - b)^2 = a + b \qquad (3)$$

Les nombres entiers a et b vérifiant la relation (3) satisfont-ils aux relations (1) et (2)?

5° On donne le reste r de la division de a par b, calculer a et b en fonction de r sachant que la relation (3) est satisfaite et que r est différent de 0.

Application numérique : $z = 11$.

316. Soient a et b deux entiers supérieurs à l'unité et premiers entre eux.

1° On considère la progression arithmétique

$$1, \ 1 + b, \ 1 + 2b, \ \dots, \ 1 + (a - 1)b$$

a) Montrer que la différence de deux termes quelconques de cette progression n'est pas divisible par a.

b) En déduire, à l'aide d'une réduction à l'absurde, que les restes des divisions par a des termes de la progression sont tous différents.

c) En conclure que l'un de ces restes est égal à zéro et qu'il existe donc un entier x et un seul inférieur à a tel que $1 + bx$ soit divisible par a.

2° *a*) A partir de cette dernière propriété, établir qu'on peut trouver, d'une façon et d'une seule, un entier x inférieur à a et un entier y inférieur à b tels que $ay - bx = 1$.

b) De même on peut trouver, d'une façon et d'une seule, un entier x' inférieur à a et un entier y' inférieur à b tels que $bx' - ay' = 1$.

c) Montrer que les fractions $\frac{x}{y}$ et $\frac{x'}{y'}$ sont irréductibles et que l'on a :

$$\frac{x}{y} < \frac{a}{b} < \frac{x'}{y'}$$

d) Montrer que $a = x + x'$, $b = y + y'$ et $x'y - xy' = 1$.

e) Déduire de cette dernière propriété que toute fraction $\frac{\lambda}{\mu}$ comprise entre $\frac{x}{y}$ et $\frac{x'}{y'}$ est telle que $\lambda > x$, $\lambda > x'$. $\mu > y$, $\mu > y'$.

317. 1° Montrer que le carré d'un nombre entier naturel pair est un multiple de 4 et le carré d'un nombre entier impair un multiple de 4 augmenté de 1.

2° On considère trois nombres entiers a, b, c satisfaisant à

$$a^2 = b^2 + c^2 \qquad (1)$$

α) Montrer que, si a, b, c sont premiers entre eux dans leur ensemble, b et c sont l'un pair et l'autre impair, et a est impair.

β) a, b, c étant premiers entre eux dans leur ensemble et b étant celui des deux nombres b et c qui est pair, montrer que $a + b$ et $a - b$ sont premiers entre eux et sont les carrés de deux nombres entiers impairs m et n premiers entre eux.

Exprimer a, b, c en fonction de m et n.

3° Donner des formules générales fournissant toutes les solutions de l'équation (1) en nombres entiers non nécessairement premiers entre eux dans leur ensemble. (On fera intervenir leur plus grand commun diviseur δ).

Indiquer toutes les solutions formées de nombres au plus égaux à 20.

318. Étant donné une fraction irréductible $\frac{a}{b} < 1$, montrer qu'elle peut se mettre sous la forme

$$\frac{a}{b} = \frac{1}{q} - \frac{r}{bq}, \quad (r < a).$$

En déduire :

$$\frac{a}{b} = \frac{1}{q} - \frac{1}{q_1} + \frac{1}{q_2} - \cdots + (-1)^n \cdot \frac{1}{q_n},$$

les fractions étant en nombre limité.

Appliquer à $\frac{a}{b} = \frac{21}{26}$.

319. 1° Démontrer que si deux nombres entiers a et b sont premiers entre eux, la fraction $\frac{a^2 b^2}{a^2 + b^2}$ est irréductible.

2° Application : déterminer deux nombres connaissant leur plus petit commun multiple 360 et la somme de leurs carrés 5409.

320. 1° Chercher toutes les valeurs du reste de la division de a^4 par 5, quand l'entier a prend toutes les valeurs possibles.

2° Démontrer que :

$$(\forall a) \qquad a^5 - a = 0, \quad \text{mod } 10$$

3° On considère deux entiers a et b ($a > b$) tels que a^5 et b^5 aient le même chiffre des unités; montrer que $a - b$ est divisible par 10, et que $a^2 - b^2$ est divisible par 20.

4° Les hypothèses du 3° étant maintenues, calculer a et b sachant que $a^2 - b^2 = 1940$.

Même question pour $a^2 - b^2 = 1920$; on vérifiera que, dans ce dernier cas, le problème admet plusieurs solutions, et on donnera toutes les solutions.

321. On considère le nombre $N = \overline{cdu}$.

Déterminer les trois chiffres c, d, u dans chacun des cas suivants :

1° $u = c$, et le nombre N est divisible par 5 et par 3.

$u = c$, et le nombre N est divisible par 3 et par 11.

3° Le nombre N est divisible par 3, 5 et 11.

4° Le nombre N est un carré parfait et est divisible par 3 et par 5.

322. 1° Démontrer que, pour satisfaire à l'égalité $\frac{A}{9} - \frac{B}{4} = 3$, A et B étant des entiers, il faut prendre A et B de la forme

$$B = 4k, \quad A = 9(k+3) \quad (k \in N)$$

2° Démontrer que le plus grand commun diviseur D de A et B ne peut être qu'un diviseur de 108.

3° Comment choisir k de façon que

a) D ne contienne pas le facteur 2;

b) D contienne le facteur 2, ou le facteur 2^2;

c) D ne contienne pas le facteur 3;

d) D contienne le facteur 3, ou le facteur 3^2, ou le facteur 3^3 ?

4° Comment choisir A et B de façon que ces nombres admettent 18 pour P.G.C.D. ?

323. Le nombre entier a étant donné, on considère deux entiers x et y supérieurs à $2a$ et tels que

$$(x - 2a)(y - 2a) = 2a^2 \qquad (1)$$

1° Montrer que tout diviseur commun des nombres $x - 2a$ et $y - 2a$ divise x et y.

2° Après avoir vérifié que la relation (1) peut s'écrire :

$$x^2 + y^2 = (x + y - 2a)^2 \qquad (2)$$

montrer que, réciproquement, tout diviseur commun des nombres x et y divise $x - 2a$ et $y - 2a$.

3° Tout diviseur commun des nombres x et y divise a.

4° En supposant $a = 30$, déterminer les couples de nombres $x; y$, premiers entre eux qui satisfont à la relation (1).

324. La fraction $\frac{a}{b}$ est supposée irréductible, et l'on désigne par $\frac{c}{d}$ la fraction irréductible qui est équivalente à la fraction

$$A = \frac{6a - 13b}{5a - 17b}.$$

1° Vérifier que $\frac{a}{b}$ est la fraction irréductible équivalente à la fraction

$$B = \frac{17c - 13d}{5c - 6d}.$$

2° Soit n le P.G.C.D. des deux termes de la fraction A et n' le P.G.C.D. des deux termes de la fraction B.

Exprimer c et d au moyen des nombres a, b, n; exprimer a et b au moyen des nombres c, d, n'; reporter dans l'expression obtenue pour c, par exemple, les expressions obtenues pour a et b. Conclure du résultat obtenu que l'une des deux fractions A et B est toujours irréductible, tandis que l'autre a ses deux termes divisibles par le nombre

$$6 \times 17 - 5 \times 13 = 37.$$

3° On a rencontré dans ce qui précède l'identité

$$6(17c - 13d) - 13(5c - 6d) = 37c$$

et on aurait de même l'identité

$$17(6a - 13b) - 13(5a - 17b) = 37a.$$

En conclure que, si l'un des deux termes de l'une des fractions A et B est divisible par 37, le second terme de la même fraction l'est aussi. L'un des termes de l'autre fraction peut-il alors être divisible par 37 ?

325. 1° Si a et b sont deux nombres entiers et si b n'est pas carré parfait, $(a + \sqrt{b})^n$, $(n \in \mathrm{N})$ peut se mettre sous la forme $A_n + B_n\sqrt{b}$, A_n et B_n appartenant à N.

2° Vérifier les égalités

$$A_{n+1} = a \cdot A_n + b \cdot B_n$$
$$B_{n+1} = A_n + a \cdot B_n.$$

Se servir de ces égalités pour calculer A_7 et B_7 en prenant $a = 3$ et $b = 5$.

3° Montrer que $(a - \sqrt{b})^n = A_n - B_n\sqrt{b}$ si a^2 est supérieur à b.

4° Si a est la valeur approchée à une unité près par excès de $\sqrt{b}$, A_n est la valeur approchée à une unité près par excès de $B_n\sqrt{b}$.

326. On considère deux fractions $\frac{a}{b}$ et $\frac{a'}{b}$ qui ont même dénominateur et dont la somme est égale à 1.

1° Que faut-il faire pour reconnaître si elles sont réduites au plus petit dénominateur commun ? Appliquer aux fonctions $\frac{1513}{5797}$ et $\frac{4284}{5797}$.

2° Démontrer que, si la fraction $\frac{a}{b}$ n'est pas convertible en fraction décimale, la fraction $\frac{a'}{b}$ ne l'est pas non plus.

3° Supposant la fraction $\frac{a}{b}$ non convertible en fraction décimale, on effectue, d'une part la division de a par b, d'autre part, celle de a' par b. Démontrer que, si l'on considère, dans chacun des deux quotients (quotients dont la partie entière est 0), le chiffre qui suit immédiatement la virgule, la somme de ces chiffres est égale à 9 et que, si l'on considère, dans chacune des deux divisions, le premier reste partiel, la somme de ces restes partiels est égale à b.

327. 1° $u(\mathrm{N})$, représentant le chiffre des unités du nombre entier N, on considère un nombre donné par son développement décimal dont la décimale de rang n après la virgule a pour valeur $u(2n + 1)$.

Ce nombre est-il périodique et, si oui, quelle est sa période ?

2° Mêmes questions avec $u(n^2 + n)$, $u(n^5 - n)$, $u\,n\,!)$, $u\left(\frac{n(n + 1)}{2}\right)$.

3° Calculer la somme et la différence des nombres donnés par leurs développements décimaux et dont les décimales de rang n sont respectivement $u(2n + 1)$ et $u(n^2)$.

328. Soient deux nombres entiers consécutifs n, $n + 1$ et leur somme $2n + 1$. Établir les propriétés suivantes :

1° Un seul des trois nombres est multiple de 3.

2° Le produit $P(n) = n(n + 1)(2n + 1)$ est multiple de 6 et sa différence avec le produit $P(n - 1)$ est égale à $6n^2$.

Peut-on déduire de là un mode de calcul de la somme S_2 des carrés des n premiers nombres entiers ?

3° Le carré de la somme $(2n + 1)^2$, est la somme de deux entiers consécutifs tels que le plus grand est la somme de deux carrés, en relation simple avec n et $n + 1$.

4° Dans la division (euclidienne dans N) du carré de la somme des carrés des deux nombres, $[n^2 + (n-1)^2]^2$, par le carré du double du grand nombre, $[2(n+1)]^2$ le quotient et le reste sont aussi des carrés.

5° Si n est un carré, le reste de la division précédente est alors le carré qui suit immédiatement le quadruple du quotient.

329. n désignant un entier positif, on considère la suite des nombres u_1, u_2, ... u_n, ... définis par

$$u_1 = u_2 = 1 \text{ et, pour } n > 2, \text{ par } u_n = u_{n+1} + 2u_{n-2}.$$

1° Montrer que tous les nombres u sont impairs. Prouver que, quel que soit n, u_n et u_{n+1} sont premiers entre eux, ainsi que u_n et u_{n+2}.

2° Prouver que, quels que soient les entiers n et p, $(p > 1)$, on a :

$$u_{n+p} = u_{n+1} \cdot u_p + 2\, u_n \cdot u_{p-1}.$$

3° Trouver le P.G.C.D. de u_n et u_{n+3}.

330. On considère l'ensemble G des nombres complexes $z = x + iy$, x et y étant des entiers rationnels $(x \in Z;\ y \in Z)$.

1° Montrer que G, muni de l'addition et de la multiplication des complexes, est un anneau.

2° Quels sont les éléments de G qui sont inversibles.

3° Soit $a = 1 + i$. Montrer que $z \in G$ s'écrit de façon unique sous la forme $z = X + Y\alpha$. Calculer X et Y en fonction de x et y.

LIVRE III

ESPACES VECTORIELS ET ALGÈBRES

CHAPITRE XXVIII

ESPACE VECTORIEL DES SUITES FINIES

351. Suites finies.

On considère les suites de n nombres, réels, ou complexes, ou entiers modulo p :

$$\{ x_1 ; x_2 ; \ldots ; x_n \}.$$

Plus particulièrement, on utilisera ici les suites de trois éléments :

$$A = \{ x ; y ; z \}$$

ou des suites de deux éléments :

$$A = \{ x ; y \}.$$

On peut aussi appeler suite à un élément un nombre x et noter :

$$A = \{ x \}.$$

La théorie qui va suivre est valable pour les suites à n *éléments; cependant on utilisera* n = 3, *dans un but de simplification qui ne réduit en rien la généralité du raisonnement.*

Si les éléments de la suite appartiennent au corps K, (K = Q, K = R, ou K = Z/p, p premier) l'ensemble des suites à n éléments est noté K^n.

352. Addition des suites de K^n.

Soient deux suites :

$$A = (x ; y ; z) \qquad \text{et} \qquad B = (x' ; y' ; z').$$

On appelle somme de ces deux suites, la suite S :

$$S = (x + x' ; y + y' ; z + z').$$

On note :

$$S = A + B.$$

◇ *Exemple.*

Soient les suites de Q^2 :

$$A = \left(-2; \frac{1}{2}\right) \quad \text{et} \quad B = \left(3; -\frac{3}{2}\right).$$

Calculer $A + B$.

La définition précédente donne :

$$A + B = (1; -1).$$

353. Propriétés de l'addition des suites finies.

L'addition des suites possède les propriétés suivantes :

Commutativité.

Soient les suites :

$$A = (x; y; z) \quad \text{et} \quad B = (x'; y'; z')$$

On a :

$$A + B = (x + x'; y + y'; z + z')$$

et

$$\begin{aligned} B + A &= (x' + x; y' + y; z' + z) \\ &= (x + x'; y + y'; z + z') \end{aligned}$$

Les deux résultats sont identiques; donc :

[C] $$(\forall A)(\forall B) : \quad A + B = B + A. \qquad (353; 1)$$

Et :

L'addition des suites est commutative.

Associativité.

Soient les suites :

$$A = (x; y; z) \qquad B = (x'; y'; z') \qquad C = (x''; y''; z'')$$

On a :

$$\begin{aligned} (A + B) + C &= (x + x'; y + y'; z + z') + (x''; y''; z'') \\ &= [(x + x') + x''; (y + y') + y''; (z + z') + z''] \end{aligned}$$

et

$$\begin{aligned} A + (B + C) &= (x; y; z) + (x' + x''; y' + y''; z' + z'') \\ &= [x + (x' + x''); y + (y' + y''); z + (z' + z'')] \end{aligned}$$

Les deux résultats sont identiques; donc :

[A] $$(\forall A)(\forall B)(\forall C) : \quad (A + B) + C = A + (B + C). \qquad (353; 2)$$

Et :

L'addition des suites est associative.

Existence d'une suite neutre.

Soit la suite :

$$A = (x;\ y;\ z)$$

On envisage la suite :

$$e = (0;\ 0;\ 0)$$

On a :

$$\begin{aligned} A + e &= (x + 0;\ y + 0;\ z + 0) \\ &= (x;\ y;\ z) \\ &= A. \end{aligned}$$

En tenant compte de la commutativité; on a :

$\boxed{N}$ $\quad (\exists e)\,(\forall A) : \quad A + e = e + A = A. \qquad$ (353 ; 3)

La loi étant additive, on note : $e = 0$.

La suite $0 = (0;\ 0;\ 0)$ *est la suite nulle*. Donc :

$(\forall A) \qquad A + 0 = 0 + A = A. \qquad$ (353 ; 4)

L'ensemble K^3 est symétrisé pour l'addition.

Soit la suite :

$$A = (x;\ y;\ z)$$

On considère la suite :

$$A' = (-\ x;\ -\ y;\ -\ z)$$

On a :

$$\begin{aligned} A + A' &= (x + (-\ x);\ y + (-\ y);\ z + (-\ z)) \\ &= (0;\ 0;\ 0) \\ &= 0. \end{aligned}$$

En tenant compte de la commutativité, on a :

$\boxed{S}$ $\quad (\forall A)\,(\exists A') : \quad A + A' = A' + A = 0. \qquad$ (353 ; 5)

Et :

Toutes les suites ont une suite symétrique pour l'addition.

On note $A' = -\ A$; et $-\ A$ est la *suite opposée de la suite A.*

354. Groupe additif des suites finies.

L'ensemble K^3 des suites de trois éléments muni de l'addition définie ci-dessus est un groupe commutatif, car l'addition possède les propriétés $\boxed{A}$ $\boxed{N}$ $\boxed{S}$ $\boxed{C}$.

Donc :

Les suites finies forment un groupe additif commutatif.

355. Régularité.

Soient trois suites A, B et M.

On suppose que l'on a :

$$A + M = B + M$$

En ajoutant $-$ M aux deux membres de cette égalité, on obtient :

$$(A + M) + (-M) = (B + M) + (-M)$$

ou

$$A + [M + (-M)] = B + [M + (-M)]$$

ou

$$A + 0 = B + 0$$

ou

$$A = B$$

Donc :

$$(\forall A)(\forall B)(\forall M) : \quad A + M = B + M \Rightarrow A = B. \qquad (355; 1)$$

Et :

Toutes les suites finies sont régulières pour l'addition.

356. Soustraction.

Soient $A \in K^3$ *et* $B \in K^3$.

Trouver la suite $X \in K^3$ *telle que*

$$A = B + X$$

s'appelle soustraire B de A.

En ajoutant $-$ B aux deux membres de l'égalité précédente, on obtient :

$$\begin{aligned}(-B) + A &= (-B) + (B + X)\\ &= [(-B) + B] + X\\ &= 0 + X\\ &= X.\end{aligned}$$

La suite cherchée est donc :

$$X = (-B) + A$$

ou

$$X = A + (-B)$$

Et :

Pour soustraire une suite on ajoute son opposée.

La suite X est la suite-différence entre A et B. On la note :

$$X = A - B$$

D'où :

$$A - B = A + (-B)$$

357. Multiplication d'une suite par un scalaire.

Soit la suite de $E = K^3$.

$$A = (x; y; z)$$

On considère un nombre λ appartenant au corps K.

On appelle produit de la suite A par le nombre λ, la suite P :

$$\mathbf{P = (\lambda x; \lambda y; \lambda z).}$$

On note :

$$P = \lambda \cdot A$$

Donc :

$$\lambda \cdot (x; y; z) = (\lambda x; \lambda y; \lambda z)$$

On définit ainsi une loi externe.

$$f: \quad (\lambda; A) \in K \times E \longrightarrow f(\lambda; A) = \lambda \cdot A \in E.$$

Le nombre $\lambda \in K$ est appelé un scalaire ou un opérateur. K est le corps des scalaires ou le corps des opérateurs.

◇ *Exemple 1.*

Soit l'ensemble $E = C^3$ des suites de trois éléments complexes.

On considère la suite :

$$A = (1 + i; -1; i)$$

et le nombre $\lambda = 1 - i \in C$.

Calculer $\lambda \cdot A$.

On a :

$$\lambda.A = (1 - i) \cdot (1 + i; -1; i)$$
$$= (1 - i^2; -1 + i; i - i^2)$$

ou

$$\lambda.A = (2; -1 + i; 1 + i).$$

◇ *Exemple 2.*

Soit l'ensemble $E = K^3$ *avec* $K = Z/5$.

On considère la suite :

$$A = (\dot{2}; -\dot{3}; \dot{4})$$

et le scalaire $\lambda = \dot{3} \in K$.

Calculer $\lambda \cdot A$.

On a :

$$\begin{aligned}\lambda A &= \dot{3} \cdot (\dot{2}; -\dot{3}; \dot{4}) \\ &= (\dot{2} \cdot \dot{3}; \dot{3} \times -\dot{3}; \dot{3} \cdot \dot{4}) \\ &= (\dot{1}; -\dot{4}; \dot{2}) \\ &= (\dot{1}; \dot{1}; \dot{2}).\end{aligned}$$

358. Propriétés de la multiplication d'une suite par un nombre.

La multiplication d'un suite par un scalaire possède les propriétés suivantes :

Neutralité.

On a :

$$\begin{aligned}1 \cdot A &= 1 \cdot (x; y; z) \\ &= (x; y; z) \\ &= A.\end{aligned}$$

D'où :

N $\qquad (\forall A) \quad 1 \times A = A. \qquad$ (358;1)

Distributivité par rapport à l'addition des suites.

Soient le nombre λ et les suites

$$A = (x; y; z) \qquad \text{et} \qquad B = (x'; y'; z')$$

On a :

$$\begin{aligned}\lambda \cdot (A + B) &= \lambda \cdot (x + x'; y + y'; z + z') \\ &= (\lambda x + \lambda x'; \lambda y + \lambda y'; \lambda z + \lambda z')\end{aligned}$$

et

$$\begin{aligned}\lambda \cdot A + \lambda \cdot B &= (\lambda x, \lambda y; \lambda z) + (\lambda x'; \lambda y'; \lambda z') \\ &= (\lambda x + \lambda x'; \lambda y + \lambda y'; \lambda z + \lambda z')\end{aligned}$$

Les deux résultats sont identiques; donc :

D' $\qquad (\forall \lambda)\,(\forall A)\,(\forall B) : \quad \lambda(A + B) = \lambda A + \lambda B. \qquad$ (358; 2)

Et :

La multiplication d'une suite par un scalaire est distributive pour l'addition des suites.

Distributivité par rapport à l'addition des scalaires.

Soient les nombres $\lambda \in K$, $\mu \in K$ et la suite

$$A = (x;\ y;\ z)$$

On a :

$$(\lambda + \mu) \cdot A = (\lambda + \mu) \cdot (x;\ y;\ z)$$
$$= (\lambda x + \mu x;\ \lambda y + \mu y;\ \lambda z + \mu z)$$

et

$$\lambda \cdot A + \mu \cdot A = (\lambda x;\ \lambda y;\ \lambda z) + (\mu x;\ \mu y;\ \mu z)$$
$$= (\lambda x + \mu x;\ \lambda y + \mu y;\ \lambda z + \mu z)$$

Les deux résultats sont identiques; donc :

[D''] $(\forall \lambda)\,(\forall \mu)\,(\forall A) :\quad (\lambda + \mu) \cdot A = \lambda \cdot A + \mu \cdot A$ (358 ; 3)

Et :

La multiplication d'une suite par un scalaire est distributive pour l'addition des scalaires.

Associativité mixte.

Soient les nombres $\lambda \in K$, $\mu \in K$ et la suite $A = (x;\ y;\ z)$.

On a :

$$\lambda\,(\mu \cdot A) = \lambda(\mu x;\ \mu y;\ \mu z)$$
$$= (\lambda\mu x;\ \lambda\mu y;\ \lambda\mu z)$$

et

$$(\lambda\mu) \cdot A = \lambda\mu \cdot (x;\ y;\ z)$$
$$= (\lambda\mu x;\ \lambda\mu y;\ \lambda\mu z)$$

Les deux résultats sont identiques; donc :

[A'] $(\forall \lambda)\,(\forall \mu)\,(\forall A) :\quad \lambda\,(\mu \cdot A) = (\lambda\mu) \cdot A.$ (358 ; 4)

359. L'espace vectoriel K^3.

L'ensemble K^3 des suites de trois éléments est muni d'une loi de composition interne notée additivement, et douant K^3 d'une structure de groupe commutatif, c'est-à-dire possédant les propriétés suivantes :

[A] $(\forall A)\,(\forall B)\,(\forall C)\quad (A + B) + C = A + (B + C).$

[N] $(\forall A)\quad A + 0 = 0 + A.$

[S] $(\forall A)(\exists(-A))$ $\quad A + (-A) = (-A) + A = 0.$

[C] $(\forall A)(\forall B)$ $\quad A + B = B + A.$

L'ensemble K^3 est muni d'une loi de composition externe, qui possède les propriétés suivantes :

[N'] $(\forall A)$ $\quad 1 \cdot A = A.$

[D'] $(\forall \lambda)(\forall A)(\forall B)$ $\quad \lambda \cdot (A + B) = \lambda A + \lambda \cdot B.$

[D''] $(\forall \lambda)(\forall \mu)$ $\quad (\lambda + \mu) \cdot A = \lambda \cdot A + \mu \cdot A.$

[A'] $(\forall \lambda)(\forall \mu)(\forall A)$ $\quad \lambda \cdot (\mu \cdot A) = (\lambda\mu) \cdot A.$

On traduit le fait que l'addition dans K^3 possède les propriétés [A] [N] [S] [C], que la loi externe possède les propriétés [N'] [D'] [D''] [A'], en disant que K^3 muni de ces deux lois a une structure d'espace vectoriel sur le corps K.

K^3 est l'espace vectoriel des suites à trois éléments du corps K.

Les suites de K^3 sont alors les vecteurs de cet espace vectoriel. Les nombres x, y, z sont les coordonnées canoniques du vecteur.

360. Autres propriétés.

1° On a :

$$\boldsymbol{0 \cdot A = 0} \qquad (360;1)$$

car

$$0 \cdot (x;y;z) = (0;0;0).$$

2° On a :

$$\lambda \cdot \boldsymbol{0} = \boldsymbol{0} \qquad (360;2)$$

car

$$\lambda \cdot (0;0;0) = (0;0;0).$$

361. Intégrités.

1° On a l'implication :

$$\boldsymbol{(\lambda \neq 0 \quad \text{et} \quad \lambda \cdot A = 0) \Rightarrow (A = 0).} \qquad (361;1)$$

En effet en multipliant $\lambda \cdot A = 0$ par $\frac{1}{\lambda}$, on obtient :

$$\frac{1}{\lambda} \cdot (\lambda \cdot A) = \frac{1}{\lambda} \cdot 0$$

ou

$$\left(\frac{1}{\lambda}\cdot\lambda\right)\cdot A = 0$$

ou

$$1 \times A = 0$$

ou

$$A = 0.$$

2° On a l'implication :

$$\textbf{(}\boldsymbol{A \neq 0} \quad \textbf{et} \quad \lambda\cdot \boldsymbol{A = 0}\textbf{)} \quad \Rightarrow \quad \textbf{(}\lambda = \boldsymbol{0}\textbf{)}. \qquad (361\,;\,2)$$

En effet :

$$\lambda\cdot A = 0$$

s'écrit :

$$(\lambda x\,;\lambda y\,;\lambda z) = (0\,;0\,;0).$$

D'où :

$$\begin{cases} \lambda x = 0 \\ \lambda y = 0 \\ \lambda z = 0 \end{cases}$$

Puisque la suite A n'est pas nulle, l'un au moins des nombres x, y, z n'est pas nul; ce qui entraîne $\lambda = 0$.

362. Régularités.

1° On a l'implication :

$$\textbf{(}\boldsymbol{A \neq 0} \quad \textbf{et} \quad \lambda\cdot \boldsymbol{A} = \mu\cdot \boldsymbol{A}\textbf{)} \quad \Rightarrow \quad \textbf{(}\lambda = \mu\textbf{)}. \qquad (362\,;\,1)$$

En effet de :

$$\lambda\cdot A = \mu\cdot A$$

on tire :

$$\lambda\cdot A - \mu\cdot A = 0$$

ou

$$(\lambda - \mu)\cdot A = 0.$$

D'après le second théorème d'intégrité, puisque $A \neq 0$, on a:

$$\lambda - \mu = 0$$

ou

$$\lambda = \mu.$$

Et :

Une suite quelconque non nulle est régulière pour la multiplication d'une suite par un scalaire.

2° On a l'implication :

$$\textbf{(}\lambda \neq \boldsymbol{0} \quad \textbf{et} \quad \lambda\cdot \boldsymbol{A} = \lambda\cdot \boldsymbol{B}\textbf{)} \quad \Rightarrow \quad \textbf{(}\boldsymbol{A = B}\textbf{)}. \qquad (362\,;\,2)$$

En effet de :

$$\lambda \cdot A = \lambda \cdot B$$

on tire :

$$\lambda A - \lambda B = 0$$

ou

$$\lambda(A - B) = 0.$$

D'après le premier théorème d'intégrité, puisque $\lambda \neq 0$, on a :

$$A - B = 0$$

ou

$$A = B.$$

Et :

Un scalaire quelconque non nul est régulier pour la multiplication d'une suite par un scalaire.

CHAPITRE XXIX

ESPACE VECTORIEL DES MATRICES UNICOLONNES

363. Matrices à une colonne.

On considère les suites de n nombres d'un corps K (K = Q; K = R, K = C, K = Z/p), $(X_1; X_2; ...; X_n)$ et on dispose ces suites verticalement :

$$\begin{pmatrix} X_1 \\ X_2 \\ \dots \\ X_n \end{pmatrix}$$

On obtient ainsi des matrices à une colonne et n lignes.

Généralement, on utilise des matrices unicolonnes à trois lignes :

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

ou des matrices unicolonnes à deux lignes :

$$\begin{pmatrix} X \\ Y \end{pmatrix}$$

On peut aussi appeler matrice à une colonne et une ligne un nombre X et noter

$$(X)$$

La théorie qui va suivre est valable pour les matrices unicolonnes quelconques; cependant on utilisera, n = 3, *dans un but de simplification qui ne réduit en rien la généralité du raisonnement.*

On désigne par E = $\mathcal{M}_1^3$ l'ensemble des matrices unicolonnes à trois lignes.

364. Addition des matrices.

Soient deux matrices

$$A = \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix}$$

On appelle somme de ces deux matrices la matrice S.

$$S = \begin{pmatrix} X + X' \\ Y + Y' \\ Z + Z' \end{pmatrix}$$

On note :

$$S = A + B.$$

Donc :

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} + \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix} = \begin{pmatrix} X + X' \\ Y + Y' \\ Z + Z' \end{pmatrix}$$

◇ *Exemple.*

Soient les matrices complexes

$$A = \begin{pmatrix} 1 + i \\ 2i \\ -2 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} -2 + 3i \\ -4 + i \\ -i \end{pmatrix}$$

Calculer $A + B$.

La définition précédente donne immédiatement

$$A + B = \begin{pmatrix} -1 + 4i \\ -4 + 3i \\ -2 - i \end{pmatrix}$$

365. Propriétés de l'addition.

L'addition des matrices unicolonnes possède les propriétés suivantes :

Commutativité.

Soient les matrices :

$$A = \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix}$$

On a :

$$A + B = \begin{pmatrix} X + X' \\ Y + Y' \\ Z + Z' \end{pmatrix}$$

et

$$B + A = \begin{pmatrix} X' + X \\ Y' + Y \\ Z' + Z \end{pmatrix}$$

Les deux résultats sont identiques; donc

C $$(\forall A)(\forall B) : \quad A + B = B + A. \qquad (365;1)$$

Et :

L'addition des matrices unicolonnes est commutative.

Associativité.

Soient les matrices :

$$A = \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \qquad B = \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix} \qquad C = \begin{pmatrix} X'' \\ Y'' \\ Z'' \end{pmatrix}$$

On a :

$$(A + B) + C = \begin{pmatrix} X + X' \\ Y + Y' \\ Z + Z' \end{pmatrix} + \begin{pmatrix} X'' \\ Y'' \\ Z'' \end{pmatrix} = \begin{pmatrix} (X + X') + X'' \\ (Y + Y') + Y'' \\ (Z + Z') + Z'' \end{pmatrix}$$

et

$$A + (B + C) = \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} + \begin{pmatrix} X' + X'' \\ Y' + Y'' \\ Z' + Z'' \end{pmatrix} = \begin{pmatrix} X + (X' + X'') \\ Y + (Y' + Y'') \\ Z + (Z' + Z'') \end{pmatrix}$$

Les deux résultats sont identiques; donc :

A $$(\forall A)(\forall B)(\forall C) : \quad (A + B) + C = A + (B + C). \qquad (365;2)$$

Et :

L'addition des matrices unicolonnes est associative.

Existence d'une matrice neutre.

Soit la matrice :

$$A = \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

On envisage la matrice :

$$e = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

On a

$$A + e = \begin{pmatrix} X + 0 \\ Y + 0 \\ Z + 0 \end{pmatrix}$$

$$= \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

$$= A.$$

En tenant compte de la commutativité, on a :

$\boxed{N}$ $$(\exists e)\ (\forall A) \qquad A + e = e + A = A \qquad (365;\ 3)$$

La loi étant additive, on note :

$$e = 0.$$

La matrice :

$$0 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

est la matrice nulle.

Donc :

$$(\forall A) \qquad A + 0 = 0 + A = 0. \qquad (365;\ 4)$$

L'ensemble $\mathcal{M}_1^3$ est symétrisé pour l'addition.

Soit la matrice :

$$A = \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

On considère la matrice :

$$A' = \begin{pmatrix} -X \\ -Y \\ -Z \end{pmatrix}$$

On a :

$$A + A' = \begin{pmatrix} X + (-X) \\ Y + (-Y) \\ Z + (-Z) \end{pmatrix}$$

$$= \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$= 0.$$

En tenant compte de la commutativité, on a :

S $(\forall A)(\exists A') : \quad A + A' = A' + A = 0.$ (365; 5)

Et :

Toutes les matrices à une colonne ont une matrice symétrique pour l'addition.

On note : $A' = -A$; et $-A$ est *l'opposée de la matrice A.*

366. Groupe additif des matrices unicolonnes.

L'ensemble M_1^3 des matrices unicolonnes muni de l'addition précédente est un groupe commutatif, car l'addition possède les propriétés A N S C.

Donc :

Les matrices unicolonnes forment un groupe additif commutatif.

367. Régularité.

Soient trois matrices A, B et M.

On suppose que l'on a

$$A + M = B + M$$

En ajoutant $-M$ aux deux membres de cette égalité, on obtient :

$$(A + M) + (-M) = (B + M) + (-M)$$

ou $$A + [M + (-M)] = B + [M + (-M)]$$

ou $$A + 0 = B + 0$$

ou $$A = B$$

Donc :

$(\forall A)(\forall B)(\forall M) : \quad A + M = B + M \Rightarrow A = B$ (565; 1)

Et :

Toutes les matrices unicolonnes sont régulières pour l'addition.

368. Soustraction.

Soient A $\in \mathcal{M}_1^3$ ***et B*** $\in \mathcal{M}_1^3$.

Trouver la matrice X telle que

$$A = B + X$$

s'appelle soustraire B de A.

En ajoutant $-$ B aux deux membres de l'égalité précédente, on obtient :

$$\begin{aligned}(-B) + A &= (-B) + (B + X)\\ &= [(-B) + B] + X\\ &= 0 + X\\ &= X.\end{aligned}$$

La matrice cherchée est donc :

$$X = A + (-B)$$

Et :

Pour soustraire une matrice on ajoute son opposée.

La matrice X est la matrice-différence entre A et B. On la note :

$$X = A - B$$

D'où :

$$A - B = A + (-B)$$

369. Multiplication d'une matrice par un scalaire.

Soit la matrice :

$$A = \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

dont les éléments *x*, *y*, *z*, appartiennent au corps K.

On considère un nombre λ appartenant au corps K.

On appelle produit de la matrice A par le nombre λ, la matrice P :

$$P = \begin{pmatrix} \lambda X \\ \lambda Y \\ \lambda Z \end{pmatrix}$$

On note :

$$P = \lambda \cdot A.$$

Donc :

$$\lambda \cdot \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} \lambda X \\ \lambda Y \\ \lambda Z \end{pmatrix}$$

On a ainsi défini une loi externe :

$$f : \quad (\lambda ; A) \in K \cdot \mathcal{M}_1^3 \rightarrow f(\lambda ; A) = \lambda A = P \in \mathcal{M}_1^3$$

Le nombre λ ∈ K est appelé un scalaire ou un opérateur. K est le corps des scalaires, ou le corps des opérateurs.

◇ *Exemple 1.*

Soient $\lambda = -2$ *et*

$$A = \begin{pmatrix} 3 \\ -2 \\ 0 \end{pmatrix}$$

Calculer $-2 \cdot A$.

On a

$$-2 \cdot A = -2 \times \begin{pmatrix} 3 \\ -2 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} -6 \\ 4 \\ 0 \end{pmatrix}$$

◇ *Exemple 2.*

Soit $\lambda = 1 + i$ *et*

$$A = \begin{pmatrix} i \\ 1 - i \\ 2 \end{pmatrix}$$

Calculer $\lambda \cdot A$.

On a :

$$(1 + i) \cdot A = (1 + i) \cdot \begin{pmatrix} i \\ 1 - i \\ 2 \end{pmatrix}$$

$$= \begin{pmatrix} i - 1 \\ 2 \\ 2 + 2i \end{pmatrix}$$

370. Propriétés de la multiplication d'une matrice par un nombre.

La multiplication d'une matrice par un nombre possède les propriétés suivantes :

Neutralité

On a :

$$1 \times A = 1 \times \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

$$= \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

D'où :

N' $$(\forall A) \qquad 1 \times A = A. \qquad (370;1)$$

Distributivité par rapport à l'addition des matrices.

Soient le nombre $\lambda \in K$ et les matrices :

$$A = \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \qquad \text{et} \qquad B = \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix}$$

On a :

$$\lambda \cdot (A + B) = \lambda \begin{pmatrix} X + X' \\ Y + Y' \\ Z + Z' \end{pmatrix} = \begin{pmatrix} \lambda X + \lambda X' \\ \lambda Y + \lambda Y' \\ \lambda Z + \lambda Z' \end{pmatrix}$$

et :

$$\lambda \cdot A + \lambda \cdot B = \begin{pmatrix} \lambda X \\ \lambda Y \\ \lambda Z \end{pmatrix} + \begin{pmatrix} \lambda X' \\ \lambda Y' \\ \lambda Z' \end{pmatrix} = \begin{pmatrix} \lambda X + \lambda X' \\ \lambda Y + \lambda Y' \\ \lambda Z + \lambda Z' \end{pmatrix}$$

Les deux résultats sont identiques; donc :

D' $$(\forall \lambda)\,(\forall A)\,(\forall B) : \quad \lambda \cdot (A + B) = \lambda A + \lambda B \qquad (370;2)$$

Et :

La multiplication d'une matrice par un scalaire est distributive pour l'addition des matrices.

Distributivité par rapport à l'addition des scalaires.

Soient les nombres $\lambda \in K$, $\mu \in K$ et la matrice

$$A = \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

On a :

$$(\lambda + \mu)\, A = (\lambda + \mu) \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} \lambda X + \mu X \\ \lambda Y + \mu Y \\ \lambda Z + \mu Z \end{pmatrix}$$

et :

$$\lambda A + \mu A = \begin{pmatrix}\lambda X\\ \lambda Y\\ \lambda Z\end{pmatrix} + \begin{pmatrix}\mu X\\ \mu Y\\ \mu Z\end{pmatrix}$$

$$= \begin{pmatrix}\lambda X + \mu X\\ \lambda Y + \mu Y\\ \lambda Z + \mu Z\end{pmatrix}$$

Les deux résultats sont identiques ; donc :

D″ $\quad (\forall\lambda)\,(\forall\mu)\,(\forall A) : \quad (\lambda + \mu)\,A = \lambda A + \mu A.$ (370 ; 3)

Et :

La multiplication d'une matrice par un scalaire est distributive pour l'addition des scalaires.

Associativité mixte.

Soient les nombres $\lambda \in K$, $\mu \in K$, et la matrice

$$A = \begin{pmatrix}X\\ Y\\ Z\end{pmatrix}$$

On a :

$$\lambda(\mu A) = \lambda \begin{pmatrix}\mu X\\ \mu Y\\ \mu Z\end{pmatrix}$$

$$= \begin{pmatrix}\lambda\mu X\\ \lambda\mu Y\\ \lambda\mu Z\end{pmatrix}$$

Et :

$$(\lambda\mu)\,A = \lambda\mu \begin{pmatrix}X\\ Y\\ Z\end{pmatrix}$$

$$= \begin{pmatrix}\lambda\mu X\\ \lambda\mu Y\\ \lambda\mu Z\end{pmatrix}$$

Les deux résultats sont identiques ; donc :

A′ $\quad (\forall\lambda)\,(\forall\mu)\,(\forall A) : \quad \lambda(\mu A) = (\lambda\mu)\,A.$ (370 ; 4)

371. L'espace vectoriel M_1^3 des matrices unicolonnes.

L'ensemble $\mathcal{M}_1^3$ des matrices à une colonne et trois lignes est muni d'une loi de composition interne , notée additivement, et, douant $\mathcal{M}_1^3$ d'une structure de groupe commutatif, c'est-à-dire possédant les propriétés suivantes :

[A] $(\forall A)(\forall B)(\forall C)$: $(A + B) + C = A + (B + C).$

[N] $(\forall A)$: $A + 0 = 0 + A = A.$

[S] $(\forall A)(\exists(-A))$: $A + (-A) = (-A) + A = 0.$

[C] $(\forall A)(\forall B)$: $A + B = B + A.$

L'ensemble $\mathcal{M}_1^3$ est muni d'une loi de composition externe, qui possède les propriétés suivantes :

[N'] $(\forall A)$: $1 \times A = A.$

[D'] $(\forall \lambda)(\forall A)(\forall B)$: $\lambda(A + B) = \lambda A + \lambda B.$

[D''] $(\forall \lambda)(\forall \mu)(\forall A)$: $(\lambda + \mu) A = \lambda A + \mu A.$

[A'] $(\forall \lambda)(\forall \mu)(\forall A)$: $\lambda(\mu A) = (\lambda\mu) A.$

On traduit le fait que l'addition dans $\mathcal{M}_1^3$, possède les propriétés [A] [N] [S] [C], que la loi externe possède les propriétés [N'] [D'] [D''] [A'], en disant que $\mathcal{M}_1^3$, muni de ces deux lois, a une structure d'espace vectoriel sur le corps K.

$\mathcal{M}_1^3$ est l'espace vectoriel des matrices à une colonne et trois lignes.

Les matrices de $\mathcal{M}_1^3$ sont alors les vecteurs de cet espace vectoriel.

372. Autres propriétés.

1° On a :

$$\boldsymbol{0 \cdot A = 0} \qquad (372; 1)$$

car

$$0 \cdot \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

2° On a :

$$\lambda \cdot \boldsymbol{0} = \boldsymbol{0} \qquad (372; 2)$$

car

$$\lambda \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

373. Intégrités.

1° On a l'implication :

$$(\lambda \neq 0 \quad \text{et} \quad \lambda \cdot A = 0) \quad \Rightarrow \quad (A = 0). \qquad (373;1)$$

En effet en multipliant $\lambda \cdot A = 0$ par $\frac{1}{\lambda}$, on obtient :

$$\frac{1}{\lambda} \cdot (\lambda \cdot A) = \frac{1}{\lambda} \cdot 0$$

ou

$$\left(\frac{1}{\lambda} \cdot \lambda\right) \cdot A = 0$$

ou

$$1 \times A = 0$$

ou

$$A = 0.$$

2° On a l'implication :

$$(A \neq 0 \quad \text{et} \quad \lambda \cdot A = 0) \quad \Rightarrow \quad (\lambda = 0). \qquad (373;2)$$

En effet :

$$(\lambda \cdot A = 0) \quad \Rightarrow \quad \lambda \cdot \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} \lambda X \\ \lambda Y \\ \lambda Z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

c'est-à-dire :

$$\begin{cases} \lambda X = 0 \\ \lambda Y = 0 \\ \lambda Z = 0 \end{cases}$$

Puisque la matrice A n'est pas nulle, l'un au moins des nombres X, Y, Z n'est pas nul; ce qui entraîne $\lambda = 0$.

374. Régularités.

1° On a l'implication :

$$(A \neq 0 \quad \text{et} \quad \lambda \cdot A = \mu A) \quad \Rightarrow \quad (\lambda = \mu) \qquad (374;1)$$

En effet de :

$$\lambda \cdot A = \mu A$$

on tire :

$$\lambda \cdot A - \mu A = 0$$

ou

$$(\lambda - \mu) A = 0.$$

D'après le second théorème d'intégrité, puisque $A \neq 0$, on a :

$$\lambda - \mu = 0$$

ou

$$\lambda = \mu.$$

Et :

Une matrice quelconque non nulle est régulière pour la multiplication d'une matrice par un scalaire.

2° On a l'implication :

$$(\lambda \neq 0 \quad \text{et} \quad \lambda \cdot A = \lambda \cdot B) \quad \Rightarrow \quad (A = B) \qquad (374; 2)$$

En effet de :

$$\lambda \cdot A = \lambda \cdot B$$

on tire :

$$\lambda \cdot A - \lambda \cdot B = 0$$

ou

$$\lambda(A - B) = 0$$

D'après le premier théorème d'intégrité, puisque $\lambda \neq 0$, on a :

$$A - B = 0$$

ou :

$$A = B.$$

Et

Un scalaire quelconque non nul est régulier pour la multiplication d'une matrice par un scalaire.

CHAPITRE XXX

DÉTERMINANTS. INDÉPENDANCE LINÉAIRE

375. Déterminant d'un bivecteur de K^2.

1° ***On appelle bivecteur de l'espace vectoriel K^2 tout couple de deux vecteurs.***

Si A et B sont les deux vecteurs, on note le bivecteur (A; B).

2° ***Soient les deux vecteurs***

$$A = (x; y) \quad \text{et} \quad B = (x'; y').$$

Le déterminant du bivecteur (A; B) est le nombre $xy' - yx$.

Ce déterminant est un déterminant d'ordre 2.

On note :

$$\text{Det}(A; B) = xy' - yx'$$

ou

$$\text{Det}(A; B) = \begin{vmatrix} x & x' \\ y & y' \end{vmatrix}$$

La première colonne du tableau

$$\begin{vmatrix} x & x' \\ y & y' \end{vmatrix}$$

est formée avec les coordonnées du vecteur A, et la seconde avec les coordonnées du vecteur B.

Le déterminant :

$$D = \begin{vmatrix} x & x' \\ y & y' \end{vmatrix}$$

se calcule donc en soustrayant du produit xy' des éléments de la diagonale descendante, le produit yx' des éléments de la diagonale montante.

◇ *Exemple 1.*

Calculer le déterminant :

$$D = \begin{vmatrix} 2 & -1 \\ 3 & -3 \end{vmatrix}$$

On a immédiatement :

$$\begin{aligned} D &= [2 \times (-3)] - [3 \times (-1)] \\ &= -6 + 3 \\ &= -3. \end{aligned}$$

◇ *Exemple 2.*

Soient les vecteurs $A = (\dot{2}; \dot{1})$ et $B = (-\dot{2}; \dot{3})$ de l'espace K^2 avec $K = Z/5$. Calculer Det (A; B).

On a :

$$\begin{aligned} \text{Det}(A; B) &= \begin{vmatrix} \dot{2} & -\dot{2} \\ \dot{1} & \dot{3} \end{vmatrix} \\ &= \dot{2} \cdot \dot{3} + \dot{1} \cdot \dot{2} \\ &= \dot{1} + \dot{2} \\ &= \dot{3}. \end{aligned}$$

376. Propriétés des déterminants d'ordre 2.

1° *Comparaison de Det (A; B) et de Det (B; A).*

On a :

$$\text{Det}(A; B) = \begin{vmatrix} x & x' \\ y & y' \end{vmatrix} = xy' - yx'$$

et

$$\text{Det}(B; A) = \begin{vmatrix} x' & x \\ y' & y \end{vmatrix} = yx' - xy'$$

Donc :

$$\textbf{Det}\,(B; A) = -\,\textbf{Det}\,(A; B). \qquad (376; 1)$$

2° *Calcul de Det $(\alpha \cdot A; \beta \cdot B)$.*

On a :

$$\begin{aligned} \text{Det}(\alpha \cdot A; \beta \cdot B) &= \begin{vmatrix} \alpha x & \beta x' \\ \alpha y & \beta y' \end{vmatrix} = \alpha\beta xy' - \alpha\beta yx' \\ &= \alpha\beta \cdot (xy' - yx'). \end{aligned}$$

Donc :

$$\textbf{Det}\,(\alpha \cdot A; \beta \cdot B) = \alpha\beta \cdot \textbf{Det}\,(A; B). \qquad (376; 2)$$

3° *Calcul de Det* $(A_1 + A_2; B)$.

On a :

$$\text{Det}(A_1 + A_2 ; B) = \begin{vmatrix} x_1 + x_2 & x' \\ y_1 + y_2 & y' \end{vmatrix}$$
$$= (x_1 + x_2)\,y' - (y_1 + y_2)\,x'.$$
$$= (x_1y' - y_1x') + (x_2y' - y_2x').$$

Donc :

$$\mathbf{Det}\,(A_1 + A_2 ; B) = \mathbf{Det}\,(A_1 ; B) + \mathbf{Det}\,(A_2 ; B). \quad (376 ; 3)$$

De même :

$$\mathbf{Det}\,(A ; B_1 + B_2) = \mathbf{Det}\,(A ; B_1) + \mathbf{Det}\,(A ; B_2). \quad (376 ; 4)$$

377. Déterminant d'un trivecteur de K^3.

1° ***On appelle trivecteur de l'espace vectoriel K^3 tout triplet de trois vecteurs.***

Si A, B et C sont les trois vecteurs, on note le trivecteur (A; B; C).

2° ***Soient les trois vecteurs***

$$A = (x; y; z) \qquad B = (x'; y'; z') \qquad C = (x''; y''; z'')$$

Le déterminant du trivecteur (A; B; C) est le nombre :

$$\mathbf{Det}\,(A;B;C) = xy'z'' + yz'x'' + zx'y'' - xz'y'' - yx'z'' - zy'x'' \quad (377; 1)$$

ou

$$\text{Det}(A ; B ; C) = \begin{vmatrix} x & x' & x'' \\ y & y' & y'' \\ z & z' & z'' \end{vmatrix}$$

Ce déterminant est un déterminant d'ordre 3.

Les colonnes du déterminant sont formées avec les coordonnées des trois vecteurs.

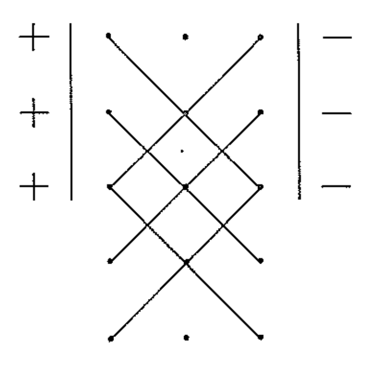
La valeur du déterminant du trivecteur (cf. formule 377; 1) s'obtient à l'aide de la règle de Sarrus. On utilise à cet effet le tableau suivant :

$$\begin{matrix} x & x' & x'' \\ y & y' & y'' \\ z & z' & z'' \\ x & x' & x'' \\ y & y' & y'' \end{matrix}$$

obtenu en écrivant au-dessous du déterminant les deux premières lignes de ce déterminant.

On calcule les trois produits des éléments des trois « diagonales descendantes » et les trois produits des éléments des trois « diagonales montantes ». De la somme des trois premiers produits on retranche la somme des trois seconds produits.

Le diagramme suivant met cette règle en évidence :

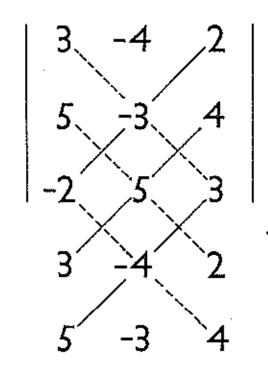


◇ *Exemple 1.*

Calculer le déterminant

$$D = \begin{vmatrix} 3 & -4 & 2 \\ 5 & -3 & 4 \\ -2 & 5 & 3 \end{vmatrix}$$

Pour utiliser la règle de Sarrus, on construit le tableau suivant :



La règle donne alors :

$$D = (3)(-3)(3) + (5)(5)(2) + (-2)(-4)(4) - (-2)(-3)(2) - (3)(5)(4) - (5)(-4)(3)$$
$$= -27 + 50 + 32 - 12 - 60 + 60$$
$$= +43.$$

◇ *Exemple 2.*

Calculer le déterminant du trivecteur $(A; B; C)$ *de l'espace vectoriel* C^3 :

$A = (1; i; 1 + i) \qquad B = (i; -1; 1 - i) \qquad C = (1 + i; 1 - i; 2)$

On a :

$$D = \text{Det}\,(A; B; C) = \begin{vmatrix} 1 & i & 1+i \\ i & -1 & 1-i \\ 1+i & 1-i & 2 \end{vmatrix}$$

La règle de Sarrus donne :

$$\begin{aligned} D &= (1)(-1)(2) + (i)(1-i)(1+i) + (1+i)(i)(1-i) \\ &\quad - (1+i)(-1)(1+i) - (1)(1-i)(1-i) - (i)(i)(2) \\ &= -2 + 2i + 2i + 2i + 2i + 2 \\ &= 8i. \end{aligned}$$

◇ *Exemple 3.*

Dans l'espace vectoriel K^3, *avec* $K = Z/5$, *on donne le trivecteur* $(A; B; C)$:

$A = (\dot{2}; -\dot{1}; \dot{3}) \qquad B = (-\dot{1}; \dot{2}; -\dot{3}) \qquad C = (\dot{3}; -\dot{2}; -\dot{1})$.

Calculer Det $(A; B; C)$.

On a :

$$\text{Det}\,(A; B; C) = \begin{vmatrix} \dot{2} & -\dot{1} & \dot{3} \\ -\dot{1} & \dot{2} & -\dot{2} \\ \dot{3} & -\dot{3} & \dot{1} \end{vmatrix}$$

La règle de Sarrus donne :

$$\begin{aligned} D &= (\dot{2})(\dot{2})(\dot{1}) + (-\dot{1})(-\dot{3})(\dot{3}) + (\dot{3})(-\dot{1})(-\dot{2}) \\ &\quad - (\dot{3})(\dot{2})(\dot{3}) - (\dot{2})(-\dot{3})(-\dot{2}) - (-\dot{1})(-\dot{1})(\dot{1}) \\ &= \dot{4} + \dot{4} + \dot{1} - \dot{3} - \dot{2} - \dot{1} \\ &= \dot{3} \end{aligned}$$

378. Propriétés des déterminants d'ordre 3.

1° *Permutation des colonnes.*

Soient les vecteurs A, B, C de K^3 On peut envisager les six permutations :

A B C	C B A
B C A	B A C
C A B	A C B

Donc on peut calculer les six déterminants :

Det (A; B; C) Det (B; C; A) Det (C; A; B)
Det (C; B; A) Det (B; A; C) Det (A; C; B)

On a, par exemple,

$$\text{Det}(B;A;C) = \begin{vmatrix} x' & x & x'' \\ y' & y & y'' \\ z' & z & z'' \end{vmatrix}$$

$$= x'yz'' + y'zx'' + z'xy'' - x'zy'' - y'xz'' - z'yx''$$
$$= -xy'z'' - yz'x'' - zx'y'' + xz'y'' + yx'y'' + zy\,x''$$

ou

$$\textbf{Det}\,(B; A; C) = -\,\textbf{Det}\,(A; B; C). \qquad (378;1)$$

On obtient ainsi :

$$\textbf{Det}\,(A; B; C) = \textbf{Det}\,(B; C; A) = \textbf{Det}\,(C; A; B) \qquad (378;2)$$

et

$$\textbf{Det}\,(C; B; A) = \textbf{Det}\,(B; A; C) = \textbf{Det}\,(A; C; B) = -\,\textbf{Det}\,(A; B; C) \qquad (378;3)$$

D'où :

Si on permute deux colonnes d'un déterminant, ce déterminant change de signe.

2° *Calcul* de Det $(\alpha A; \beta B; \gamma C)$.

On a :

$$\text{Det}(\alpha\cdot A; \beta\cdot B; \gamma\cdot C) = \begin{vmatrix} \alpha x & \beta x' & \gamma x'' \\ \alpha y & \beta y' & \gamma y'' \\ \alpha z & \beta z' & \gamma z'' \end{vmatrix}$$

$$= \alpha\beta\gamma\cdot(xy'z'' + yz'x'' + zx'y'' - xz'y'' - yx'z'' - zy'x'').$$

D'où :

$$\textbf{Det}\,(\alpha\cdot A; \beta\cdot B; \gamma\cdot C) = \alpha\beta\gamma\cdot\textbf{Det}\,(A; B; C). \qquad (378;4)$$

3° *Calcul de* Det $(A_1 + A_2; B; C)$.

On a :

$$D = \text{Det}(A_1 + A_2; B; C) = \begin{vmatrix} x_1 + x_2 & x' & x'' \\ y_1 + y_2 & y' & y'' \\ z_1 + z_2 & z' & z'' \end{vmatrix}$$

ou :

$$D = (x_1 + x_2)\,y'z'' + (y_1 + y_2)\,z'x'' + (z_1 + z_2)\,x'y'' - (x_1 + x_2)\,z'y'' - (y_1 + y_2)\,x'z'' - (z_1 + z_2)\,y'x''.$$
$$= [x_1y'z'' + y_1z'x'' + z_1x'y'' - x_1z'y'' - y_1x'z'' - z_1y'x'']$$
$$+ [x_2y'z'' + y_2z'x'' - x_2z'y'' - x_2z'y'' - y_2x'z'' - z_2y'x'']$$

D'où :

$$\textbf{Det}\,(A_1 + A_2; B; C) = \textbf{Det}\,(A_1; B; C) + \textbf{Det}\,(A_2; B; C) \qquad (378;5)$$

De même :

Det $(A; B_1 + B_2; C) =$ **Det** $(A; B_1; C) +$ **Det** $(A; B_2; C)$ (378; 6)

et

Det $(A; B; C_1 + C_2) =$ **Det** $(A; B; C_1) +$ **Det** $(A; B; C_2)$ (378; 7)

379. Combinaison linéaire de vecteurs.

Soient trois vecteurs A, B, C, appartenant à l'espace vectoriel E sur le corps K.

On appelle combinaison linéaire de ces trois vecteurs A, B, C le vecteur $P = \alpha \cdot A + \beta \cdot B + \gamma \cdot C$. α, β, γ ***appartenant au corps K.***

α, β, γ ***sont les coefficients de la combinaison linéaire.***

◇ *Exemple 1.*

On donne les vecteurs de $E = R^3$:

$$A = (2; 1; -1) \qquad B = (-2; 2; 3) \qquad C = (0; 2; -3)$$

Calculer $P = 2 \cdot A - 3 \cdot B + C$.

On obtient immédiatement :

$$\begin{aligned} P &= 2 \cdot (2; 1; -1) - 3 \cdot (-2; 2; 3) + (0; 2; -3) \\ &= (4; 2; -2) + (6; -6; -9) + (0; 2; -3) \\ &= (10; -2; -14). \end{aligned}$$

◇ *Exemple 2.*

Dans l'espace vectoriel $\mathcal{M}_1^2$ *construit sur le corps C, on donne les vecteurs*

$$A = \begin{pmatrix} 1 - i \\ i \end{pmatrix} \qquad B = \begin{pmatrix} -1 \\ 2 - i \end{pmatrix}$$

Calculer la combinaison linéaire $A - iB$.

On a immédiatement :

$$\begin{aligned} A - i \cdot B &= \begin{pmatrix} 1 - i \\ i \end{pmatrix} - i \cdot \begin{pmatrix} -1 \\ 2 - i \end{pmatrix} \\ &= \begin{pmatrix} 1 - i + i \\ i - 2i - 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 \\ -1 - i \end{pmatrix} \end{aligned}$$

◇ *Exemple 3.*

Soient les vecteurs de K^2, *avec* $K = Z/5$;

$$A = (\dot{1}; -\dot{2}) \qquad B = (-\dot{3}; \dot{4}) \qquad C = (\dot{1}; \dot{4}).$$

Calculer $P = \dot{2}A - B + \dot{3} \cdot C$.

On a immédiatement :

$$\begin{aligned} P &= \dot{2}(\dot{1}\,;-\dot{2}) - (-\dot{3}\,;\dot{4}) + \dot{3}(\dot{1}\,;\dot{4}) \\ &= (\dot{2}\,;-\dot{4}) + (\dot{3}\,;-\dot{4}) + (\dot{3}\,;\dot{2}) \\ &= (\dot{3}\,;\dot{4}). \end{aligned}$$

380. Indépendance linéaire de deux vecteurs.

1° ***Soient deux vecteurs A et B, non nuls, de l'espace vectoriel E sur le corps K.***

Ces deux vecteurs A et B sont linéairement dépendants si on peut trouver deux nombres α et β du corps K, non nuls, tels que

$$\alpha \cdot A + \beta \cdot B = 0.$$

β étant différent de zéro, on tire de la relation précédente :

$$B = -\frac{\alpha}{\beta} \cdot A$$

ou

$$B = \lambda \cdot A. \qquad (380\,;1)$$

Donc :

Deux vecteurs A et B, non nuls, sont linéairement dépendants si on peut trouver un nombre λ, non nul, tel que $B = \lambda \cdot A$.

2° *Si les vecteurs A et B ne sont pas linéairement dépendants, ils sont dits linéairement indépendants.*

381. Condition de dépendance de deux vecteurs.

Pour que les vecteurs A et B soient linéairement dépendants il faut et il suffit que

$$B = \lambda \cdot A.$$

Si $A = (x;\, y;\, z)$ et $B = (x';\, y';\, z')$, cette condition s'exprime par

$$\begin{aligned} (x';\, y';\, z') &= \lambda \cdot (x;\, y;\, z) \\ &= (\lambda x;\, \lambda y;\, \lambda z) \end{aligned}$$

ou encore par :

$$\begin{cases} x' = \lambda \cdot x \\ y' = \lambda \cdot y \\ z' = \lambda \cdot z \end{cases}$$

D'où :

$$\frac{x'}{x} = \frac{y'}{y} = \frac{z'}{z} = \lambda.$$

Par suite, on a l'équivalence :

$$[\textit{A, B, linéairement dépendants}] \quad \Leftrightarrow \quad \left[\frac{x'}{x} = \frac{y'}{y} = \frac{z'}{z}\right].$$

◇ *Exemple 1.*

Dans l'espace $\mathcal{M}_1^3$ construit sur R, on considère les vecteurs

$$A = \begin{pmatrix} 3 \\ -6 \\ 9 \end{pmatrix} \qquad \text{et} \qquad B = \begin{pmatrix} 2 \\ -4 \\ 6 \end{pmatrix}$$

Ces vecteurs sont-ils linéairement dépendants ?

On a :

$$\frac{x'}{x} = \frac{2}{3} \qquad \frac{y'}{y} = \frac{-4}{-6} = \frac{2}{3} \qquad \frac{z'}{z} = \frac{6}{9} = \frac{2}{3}.$$

Donc :

$$\frac{x'}{x} = \frac{y'}{y} = \frac{z'}{z}$$

et les vecteurs A et B sont linéairement dépendants.

De plus :

$$B = \frac{2}{3} \cdot A$$

ou

$$2 \cdot A - 3 \cdot B = 0.$$

◇ *Exemple 2.*

Soient dans R^3 les vecteurs $A = (1;\ 1;\ 3)$ et $B = (2;\ 1;\ 2)$. Etudier leur dépendance.

On a :

$$\frac{x'}{x} = 2 \qquad \frac{y'}{y} = 1 \qquad \frac{z'}{z} = \frac{2}{3}.$$

Les trois rapports ne sont pas égaux. Donc les vecteurs A et B sont linéairement indépendants.

◇ *Exemple 3.*

Soient les vecteurs de l'espace K^3, avec $K = Z/5$:

$$A = (\dot{2};\ -\dot{1};\ \dot{4}) \quad \text{et} \quad B = (\dot{3};\ \dot{1};\ \dot{1}).$$

Etudier la dépendance ou l'indépendance de ces deux vecteurs.

On a :

$$\frac{x'}{x} = \frac{\dot{3}}{\dot{2}} = \dot{3} \cdot \dot{3} = \dot{4} \qquad (\text{car } (\dot{2})^{-1} = \dot{3})$$

$$\frac{y'}{y} = \frac{\dot{1}}{-\dot{1}} = -\dot{1} = \dot{4}$$

$$\frac{z'}{z} = \frac{\dot{1}}{\dot{4}} = \dot{1} \cdot \dot{4} = \dot{4} \qquad (\text{car } (\dot{4})^{-1} = \dot{4}).$$

Donc :

$$\frac{x'}{x} = \frac{y'}{y} = \frac{z'}{z}$$

et les vecteurs A et B sont linéairement dépendants.

De plus :

$$B = \dot{4} \cdot A.$$

382. Dépendance linéaire de deux vecteurs de K^2 ou de $\mathcal{V}_1^2$.

Soient deux vecteurs de l'espace vectoriel $E = K^2$ (ou $E = \mathcal{V}_1^2$) :

$$A = (x; y) \quad \text{et} \quad B = (x'; y')$$

La condition de dépendance

$$\frac{x'}{x} = \frac{y'}{y}$$

peut s'écrire :

$$xy' - yx' = 0$$

c'est-à-dire :

$$\text{Det}\,(A; B) = 0$$

Donc :

Une condition nécessaire et suffisante pour que deux vecteurs de K^2 (ou de $\mathcal{V}_1^2$) soient linéairement dépendants est que leur déterminant soit nul.

Et :

Une condition nécessaire et suffisante pour que deux vecteurs de K^2 (ou de $\mathcal{V}_1^2$) soient linéairement indépendants est que leur déterminant ne soit pas nul.

◇ *Exemple 1.*

Soient les deux vecteurs $A = (3; -2)$ et $B = (-6; 4)$ de l'espace vectoriel R^2. Montrer qu'ils sont linéairement dépendants.

On a :

$$\begin{aligned}\text{Det}(A; B) &= \begin{vmatrix} 3 & -6 \\ -2 & 4 \end{vmatrix} \\ &= 12 - 12 \\ &= 0.\end{aligned}$$

Donc A et B sont linéairement dépendants.

◇ *Exemple 2.*

Les vecteurs :

$$A = \begin{pmatrix} -2 \\ 4 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 4 \\ 8 \end{pmatrix}$$

de l'espace vectoriel $\mathcal{M}_1^2$ sur R sont-ils dépendants ou indépendants ?

On a :

$$\begin{aligned}\text{Det}(A; B) &= \begin{vmatrix} -2 & 4 \\ 4 & 8 \end{vmatrix} \\ &= -16 - 16 \\ &= -32.\end{aligned}$$

Donc A et B sont linéairement indépendants.

◇ *Exemple 3.*

Dans C^2 on donne les vecteurs $A = (3 + i; -2)$ et $B = (-6i + 2; 4i)$. Montrer qu'ils sont linéairement dépendants.

On a :

$$\begin{aligned}\text{Det}(A; B) &= \begin{vmatrix} 3 + i & -6i + 2 \\ -2 & 4i \end{vmatrix} \\ &= 4i(3 + i) + 2(-6i + 2) \\ &= 12i - 4 - 12i + 4 \\ &= 0.\end{aligned}$$

Donc A et B sont linéairement dépendants.

383. Sens relatif de deux vecteurs dépendants d'un espace vectoriel sur le corps des réels.

Soit l'espace vectoriel $E = R^2$ (ou $E = R^3$) ou l'espace vectoriel $E = \mathcal{M}_1^2$ (ou $E = \mathcal{M}_1^3$) construit sur le corps E des réels.

Soient deux vecteurs A et B de E, linéairement dépendants. Il existe donc un nombre réel λ tel que

$$B = \lambda \cdot A.$$

Si λ est positif, les vecteurs A et B sont dits de même sens.
Si λ est négatif, les vecteurs A et B sont dits de sens contraire.

384. Indépendance linéaire de trois vecteurs.

1° ***Soient trois vecteurs A, B et C, non nuls, de l'espace vectoriel E sur le corps K.***

Ces trois vecteurs A, B et C sont linéairement dépendants si on peut trouver trois nombres α, β, γ du corps K, non tous nuls, tels que $\alpha \cdot A + \beta \cdot B + \gamma \cdot C = 0$.

Si γ n'est pas nul, on tire de cette relation :

$$C = -\frac{\alpha}{\gamma} \cdot A - \frac{\beta}{\gamma} \cdot B$$

ou

$$C = \lambda \cdot A + \mu \cdot B \qquad (384; 1)$$

Donc :

Trois vecteurs A, B, C, non nuls, sont linéairement dépendants si on peut trouver deux nombres λ et μ (non nuls tous les deux) tels que $C = \lambda \cdot A + \mu \cdot B$.

2° *Si les vecteurs A, B, C ne sont pas linéairement dépendants, ils sont dits linéairement indépendants.*

385. Dépendance linéaire de trois vecteurs de K^3 ou de $\mathcal{M}_1^3$.

Dans l'espace vectoriel K^3 (ou $\mathcal{M}_1^3$), on considère les trois vecteurs, non nuls :

$$A = (x; y; z) \qquad B = (x'; y'; z') \qquad C = (x''; y''; z'')$$

Pour que ces trois vecteurs soient linéairement dépendants il suffit qu'il existe trois nombres α, β, γ de K, non tous nuls tels, que

$$\alpha . A + \beta . B + \gamma . C = 0$$

c'est-à-dire :

$$\alpha.(x; y; z) + \beta.(x'; y'; z') + \gamma.(x''; y''; z'') = 0$$

ou

$$(\alpha x + \beta x' + \gamma x''; \alpha y + \beta y' + \gamma y''; \alpha z + \beta z' + \gamma z'') = 0$$

ou encore :

$$\begin{cases} \alpha x + \beta x' + \gamma x'' = 0 \\ \alpha y + \beta y' + \gamma y'' = 0 \\ \alpha z + \beta z' + \gamma z'' = 0 \end{cases}$$

Or si on prend :

$$\alpha = \begin{vmatrix} y' & y'' \\ z' & z'' \end{vmatrix} = y'z'' - z'y''$$

$$\beta = \begin{vmatrix} y'' & y \\ z'' & z \end{vmatrix} = zy'' - yz''$$

$$\gamma = \begin{vmatrix} y & y' \\ z & z' \end{vmatrix} = yz' - zy'.$$

On a :

$$\begin{aligned} \alpha x + \beta x' + \gamma x'' &= x(y'z'' - z'y'') + x'(zy'' - yz'') + x''(yz' - zy') \\ &= xy'z'' - xz'y'' + zx'y'' - yx'z'' + yz'x'' - zy'x'' \\ &= \text{Det }(A; B; C) \end{aligned}$$

$$\begin{aligned} \alpha y + \beta y' + \gamma y'' &= y(y'z'' - z'y'') + y'(zy'' - yz'') + y''(yz' - zy') \\ &= yy'z'' - yz'y'' + zy'y'' - yy'z'' + yz'y'' - zy'y'' \\ &= 0 \end{aligned}$$

$$\begin{aligned} \alpha z + \beta z' + \gamma z'' &= z(y'z'' - z'y'') + z'(zy'' - yz'') + z''(yz' - zy') \\ &= zy'z'' - zz'y'' + zz'y'' - yz'z'' + yz'z'' - zy'z'' \\ &= 0. \end{aligned}$$

La condition de dépendance s'exprime donc par Det (A; B; C) = 0.

D'où :

Une condition nécessaire et suffisante pour que trois vecteurs de l'espace vectoriel K^3 soient linéairement dépendants est que leur déterminant soit nul.

Et :

Une condition nécessaire et suffisante pour que trois vecteurs de l'espace vectoriel K^3 soient linéairement indépendants est que leur déterminant ne soit pas nul.

◇ *Exemple 1.*

Montrer que les vecteurs de R^3 :

$$A = (2; 1; 2) \qquad B = (-1; 1; 2) \qquad C = (1; 1; 2)$$

sont linéairement dépendants.

On a :

$$\operatorname{Det}(A;B;C)=\begin{vmatrix}2 & -1 & 1\\ 1 & 1 & 1\\ 2 & 2 & 2\end{vmatrix}$$

$$= 4 + 2 - 2 - 2 - 4 + 2$$

$$= 0.$$

De plus on a :

$$2 \cdot A + B = 3 \cdot C.$$

◇ *Exemple 2.*

Montrer que les vecteurs de R^3 :

$u = (1; 0; 1) \qquad v = (-1; 0; 1) \qquad w = (0; 1; 1)$

sont linéairement indépendants.

On a :

$$\operatorname{Det}(u;v;w)=\begin{vmatrix}1 & -1 & 0\\ 0 & 0 & 1\\ 1 & 1 & 1\end{vmatrix}$$

$$= -1 - 1$$

$$= -2.$$

Donc les vecteurs sont linéairement indépendants.

CHAPITRE XXXI

BASES D'UN ESPACE VECTORIEL[1]

386. Base canonique de K^2.

On désigne par 1 l'unité du corps K, c'est-à-dire le neutre pour la multiplication.

Dans l'espace vectoriel K^2, on envisage les vecteurs

$$i = (1;0) \quad \text{et} \quad j = (0;1).$$

Ces deux vecteurs sont linéairement indépendants; en effet leur déterminant

$$\text{Det}(i;j) = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1$$

n'est pas nul.

L'ensemble $\mathcal{B}_0 = \{ i;j \}$ de ces deux vecteurs est appelé la base canonique de l'espace vectoriel K^2.

Remarque.

Dans l'espace vectoriel $\mathcal{M}_1^2$ sur K, la base canonique est l'ensemble des deux vecteurs

$$i = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{et} \quad j = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

387. Expression d'un vecteur dans la base canonique de K^2.

Soit un vecteur quelconque $A = (x; y)$ de l'espace vectoriel K^2.

On peut écrire :

$$\begin{aligned} A &= (x; y) \\ &= (x; 0) + (0; y) \\ &= x\cdot(1; 0) + y\cdot(0; 1) \end{aligned}$$

ou

$$A = x\cdot i + y\cdot j. \qquad (387;1)$$

---

(1) La question est traitée dans K^2 (nos 386 à 395) puis dans K^3 (nos 396 à 406).

Cette expression du vecteur A par une combinaison linéaire des vecteurs de la base $\mathcal{B}_0$ est unique. En effet, soit une seconde décomposition du vecteur A dans $\mathcal{B}_0$:

$$A = x' \cdot i + y' \cdot j \qquad (387;2)$$

En soustrayant la formule (387; 2) de la formule (387; 1) on obtient :

$$(x - x') \cdot i + (y - y') \cdot j = 0$$

Comme les vecteurs i et j sont linéairement indépendants, les coefficients $x - x'$ et $y - y'$ de cette combinaison linéaire nulle sont nuls; d'où :

$$x = x' \qquad \text{et} \qquad y = y'$$

On peut alors énoncer :

Un vecteur quelconque de K^2 est une combinaison linéaire unique des vecteurs de la base canonique.

388. Base quelconque de K^2.

Dans l'espace vectoriel K^2, on envisage les vecteurs $u = (\alpha; \beta)$ et $v = (\alpha'; \beta')$ linéairement indépendants; leur déterminant n'est pas nul.

$$\text{Det}(u; v) = \begin{vmatrix} \alpha & \alpha' \\ \beta & \beta' \end{vmatrix} = \alpha\beta' - \beta\alpha' \neq 0.$$

L'ensemble $\mathcal{B} = \{ u; v \}$ de ces deux vecteurs linéairement indépendants est une base de l'espace vectoriel K^2.

D'après la formule (387; 1) on a :

$$\begin{cases} u = \alpha \cdot i + \beta \cdot j \\ v = \alpha' \cdot i + \beta' \cdot j \end{cases} \qquad (388;1)$$

Ces formules donnent les vecteurs u *et* v *de la base* $\mathcal{B}$ *en fonction des vecteurs* i *et* j *de la base canonique* $\mathcal{B}_0$.

D'autre part, on a

$$\beta' \cdot u - \beta \cdot v = \beta'(\alpha \cdot i + \beta \cdot j) - \beta(\alpha' \cdot i + \beta' \cdot j) = (\alpha\beta' - \beta\alpha') \cdot i$$

et

$$-\alpha' \cdot u + \alpha \cdot v = -\alpha'(\alpha \cdot i + \beta \cdot j) + \alpha(\alpha' \cdot i + \beta' \cdot j) = (\alpha\beta' - \beta\alpha') \cdot j$$

$\alpha\beta' - \beta\alpha'$ n'étant pas nul; on obtient :

$$\begin{cases} i = \dfrac{\beta'}{\alpha\beta' - \beta\alpha'} \cdot u - \dfrac{\beta}{\alpha\beta' - \beta\alpha'} \cdot v \\ j = -\dfrac{\alpha'}{\alpha\beta' - \beta\alpha'} \cdot u + \dfrac{\alpha}{\alpha\beta' - \beta\alpha'} \cdot v \end{cases} \qquad (388;2)$$

Ces formules donnent les vecteurs i *et* j *de la base canonique* $\mathcal{B}_0$ *en fonction des vecteurs* u *et* v *de la base* $\mathcal{B}$.

On pose pour simplifier :

$$\xi = \frac{\beta'}{\alpha\beta' - \beta\alpha'} \qquad \eta = \frac{-\beta}{\alpha\beta' - \beta\alpha'}$$

$$\xi' = \frac{-\alpha'}{\alpha\beta' - \beta\alpha'} \qquad \eta' = \frac{\alpha}{\alpha\beta' - \beta\alpha'}$$

Les formules (388; 2) s'écrivent alors :

$$\begin{cases} i = \xi \cdot u + \eta \cdot v \\ j = \xi' \cdot u + \eta' \cdot v \end{cases} \qquad (388; 3)$$

389. Expression d'un vecteur dans une base quelconque.

Dans l'espace K^2, on considère les deux bases $\mathcal{B}_0 = \{i; j\}$ et $\mathcal{B} = \{u; v\}$

En remplaçant dans

$$A = x \cdot i + y \cdot j \qquad (389; 1)$$

i et j par les formules (388; 3), on obtient :

$$\begin{aligned} A &= x(\xi \cdot u + \eta \cdot v) + y(\xi' \cdot u + \eta' \cdot v) \\ &= (\xi \cdot x + \xi' \cdot y)\, u + (\eta \cdot x + \eta' \cdot y) \cdot v \end{aligned}$$

On pose :

$$\begin{cases} X = \xi \cdot x + \xi' \cdot y \\ Y = \eta \cdot x + \eta' \cdot y \end{cases} \qquad (389; 2)$$

et :

$$A = X \cdot u + Y \cdot v. \qquad (389; 3)$$

Cette décomposition du vecteur A dans la base β est unique. En effet soit une seconde décomposition de A :

$$A = X' \cdot u + Y' \cdot v$$

Par soustraction on obtient :

$$(X - X') \cdot u + (Y - Y') \cdot v = 0$$

Comme les vecteurs u et v sont linéairement indépendants, les coefficients $X - X'$ et $Y - Y'$ de cette combinaison linéaire nulle sont nuls; d'où :

$$X = X' \qquad \text{et} \qquad Y = Y'$$

On peut alors énoncer :

Un vecteur quelconque de K^2 est une combinaison linéaire unique des vecteurs d'une base quelconque de K^2.

Les nombres X et Y sont les coordonnées du vecteur A dans la base $\mathcal{B} = \{u; v\}$

390. Changement de base.

Dans l'espace vectoriel K^2 on considère les bases

$$\mathcal{B}_0 = \{ i ; j \} \quad \text{et} \quad \mathcal{B} = \{ u ; v \}$$

la base $\mathcal{B}_0$ n'étant plus nécessairement la base canonique.

On donne :

$$\begin{cases} u = \alpha \cdot i + \beta \cdot j \\ v = \alpha' \cdot i + \beta \cdot' j \end{cases} \qquad (390;\ 1)$$

Comme au nº 388, on en déduit :

$$\begin{cases} i = \xi \cdot u + \eta \cdot v \\ j = \xi' \cdot u + \eta' \cdot v \end{cases} \qquad (390;\ 2)$$

Dans la base $\mathcal{B}_0$ on a :

$$A = x \cdot i + y \cdot j \qquad (390;\ 3)$$

et dans la base $\mathcal{B}$:

$$A = X \cdot u + Y \cdot v \qquad (390;\ 4)$$

1º Le calcul du nº 389, donne

$$\begin{cases} X = \xi \cdot x + \xi' \cdot y \\ Y = \eta \cdot x + \eta' \cdot y \end{cases} \qquad (390;\ 5)$$

Ces formules donnent les coordonnées X, Y du vecteur A dans la base $\mathcal{B}$ en fonction des coordonnées x, y du même vecteur A dans la base $\mathcal{B}_0$.

2º En remplaçant dans $A = X \cdot u + Y \cdot v$, u et v par les expressions (390; 1) on obtient :

$$\begin{aligned} A &= X \cdot (\alpha \cdot i + \beta \cdot j) + Y\,(\alpha' \cdot i + \beta' \cdot j) \\ &= (a \cdot X + \alpha' \cdot Y) \cdot i + (\beta\ X + \beta' \cdot Y) \cdot j \end{aligned}$$

En comparant à (390; 3), et par suite de l'unicité de la décomposition du vecteur A dans $\mathcal{B}_0$, on déduit

$$\begin{cases} x = \alpha \cdot X + \alpha' \cdot Y \\ y = \beta X + \beta' Y \end{cases} \qquad (390;\ 6)$$

Ces formules donnent les coordonnées x, y du vecteur A dans la base $\mathcal{B}_0$ en fonction des coordonnées X, Y du même vecteur A dans la base $\mathcal{B}$.

Les formules (390; 5) et (390; 6) sont les *formules de changement de base dans K^2.*

391. Addition des vecteurs et changement de base dans K^2.

Soient les vecteurs :

$$A = (x ; y), \qquad B = (x' ; y')$$

et leur somme :

$$S = A + B = (x + x'; y + y').$$

Ces trois vecteurs sont donnés dans la base $\mathcal{B}_0$.

Dans la base $\mathcal{B} = \{u; v\}$ les coordonnées de A et B sont X, Y et X', Y' respectivement avec

$$\begin{cases} X = \xi \cdot x + \xi' \cdot y \\ Y = \eta \cdot x + \eta' \cdot y \end{cases} \qquad \begin{cases} X' = \xi \cdot x' + \xi' \cdot y' \\ Y' = \eta \cdot x' + \eta' \cdot y' \end{cases}$$

Les coordonnées (X″; Y″) dans $\mathcal{B}$ de la somme S = A + B sont données par les formules (390; 5) :

$$\begin{cases} X'' = \xi(x + x') + \xi'(y + y') = (\xi \cdot x + \xi' \cdot y) + (\xi \cdot x' + \xi' \cdot y') = X + X' \\ Y'' = \eta(x + x') + \eta'(y + y') = (\eta \cdot x + \eta' \cdot y) + (\eta x' + \eta' y') = Y + Y' \end{cases}$$

Donc, la somme S = A + B se calcule de la même façon dans la base $\mathcal{B}$ et dans la base $\mathcal{B}_0$.

On dit que :

L'addition des vecteurs est indépendante de la base ou est intrinsèque.

392. Multiplication d'un vecteur par un scalaire et changement de base.

Soient le vecteur A = (x; y) et le scalaire λ. On considère le produit λ·A :

$$P = \lambda \cdot A = (\lambda x; \lambda y).$$

Ces vecteurs A et P sont donnés dans la base $\mathcal{B}_0$.

Dans la base $\mathcal{B} = \{u; v\}$ les coordonnées de A sont X, Y avec

$$\begin{cases} X = \xi \cdot x + \xi' \cdot y \\ Y = \eta \cdot x + \eta' \cdot y \end{cases}$$

Les coordonnées X″, Y″ dans $\mathcal{B}$ du vecteur P = λ·A sont données par les formules (390; 5) :

$$\begin{cases} X'' = \xi(\lambda \cdot x) + \xi'(\lambda \cdot y) = \lambda(\xi \cdot x + \xi' \cdot y) = \lambda \cdot X \\ Y'' = \eta(\lambda \cdot x) + \eta'(\lambda \cdot y) = \lambda(\eta \cdot x + \eta' \cdot y) = \lambda \cdot Y \end{cases}$$

Donc, le produit P = λ·A se calcule de la même façon dans la base $\mathcal{B}$ et dans la base $\mathcal{B}_0$.

Et :

La multiplication d'un vecteur par un scalaire est intrinsèque.

393. Remarque.

L'addition des vecteurs et la multiplication d'un vecteur par un scalaire étant intrinsèques, on déduit :

La dépendance linéaire et l'indépendance linéaire de plusieurs vecteurs est intrinsèque.

394. Déterminant et changement de base.

Soient les vecteurs A et B.

Dans la base $\mathcal{B}_0 = \{ i ; j \}$ on a :

$$\begin{cases} A = x \cdot i + y \cdot j \\ B = x' \cdot i + y' \cdot j \end{cases}$$

et dans la base $\mathcal{B} = \{ u ; v \}$:

$$\begin{cases} A = X \cdot u + Y \cdot v \\ B = X' \cdot u + Y' \cdot v \end{cases}$$

On note :

$$[\text{Det}\,(A ; B)]_{\mathcal{B}_0} = \begin{vmatrix} x & x' \\ y & y' \end{vmatrix}$$

et

$$[\text{Det}\,(A ; B)]_{\mathcal{B}} = \begin{vmatrix} X & X' \\ Y & Y' \end{vmatrix}$$

On a :

$$\begin{aligned} [\text{Det}\,(A; B)]_{\mathcal{B}_0} &= [\text{Det}\,(X \cdot u + Y \cdot v; B)]_{\mathcal{B}_0} \\ &= [\text{Det}\,(X \cdot u; B)]_{\mathcal{B}_0} + [\text{Det}\,(Y \cdot v; B)]_{\mathcal{B}_0} \\ &= X \cdot [\text{Det}\,(u; B)]_{\mathcal{B}_0} + Y \cdot [\text{Det}\,(v; B)]_{\mathcal{B}_0} \end{aligned}$$

Or

$$\begin{aligned} [\text{Det}\,(u; B)]_{\mathcal{B}_0} &= [\text{Det}\,(u; X' \cdot u + Y' \cdot v]_{\mathcal{B}_0} \\ &= X' \cdot [\text{Det}\,(u;u)]_{\mathcal{B}_0} + Y' \cdot [\text{Det}\,(u; v)]_{\mathcal{B}_0} \\ &= Y' \cdot [\text{Det}\,(u; v)]_{\mathcal{B}_0} \end{aligned}$$

$$\begin{aligned} [\text{Det}\,(v; B)]_{\mathcal{B}_0} &= [\text{Det}\,(v; X' \cdot u + Y' \cdot v)]_{\mathcal{B}_0} \\ &= [\text{Det}\,(v; X' \cdot u)]_{\mathcal{B}_0} + [\text{Det}\,(v; Y' \cdot v)]_{\mathcal{B}_0} \\ &= X' \cdot [\text{Det}\,(v; u)]_{\mathcal{B}_0} + Y' \cdot [\text{Det}\,(v; v)]_{\mathcal{B}_0} \\ &= - X' \cdot [\text{Det}\,(u; v)]_{\mathcal{B}_0} \end{aligned}$$

Par suite :

$$\begin{aligned} [\text{Det}\,(A; B)]_{\mathcal{B}_0} &= XY' \cdot [\text{Det}\,(u; v)]_{\mathcal{B}_0} - YX' \cdot [\text{Det}\,(u; v)]_{\mathcal{B}_0} \\ &= (XY' - YX') \cdot [\text{Det}\,(u; v)]_{\mathcal{B}_0} \end{aligned}$$

D'où la formule :

$$[\textbf{Det}\,(A; B)]_{\mathcal{B}_0} = [\textbf{Det}\,(\mathbf{u}; \mathbf{v})]_{\mathcal{B}_0} \times [\textbf{Det}\,(A; B)]_{\mathcal{B}} \qquad (394; 1)$$

Le déterminant n'est donc pas intrinsèque.

395. Orientation d'un bivecteur de R^2.

On envisage dans ce numéro l'espace vectoriel R^2 rapporté à sa base canonique $\mathcal{B}_0$.

1° Soit le bivecteur (A; B) de l'espace vectoriel R^2. Le déterminant de ce bivecteur dans la base $\mathcal{B}_0$ est $D = \text{Det}\,(A; B)$.

Si le déterminant canonique D d'un bivecteur est positif, le bivecteur est dit orienté positivement relativement à la base canonique $\mathcal{B}_0$.
Si le déterminant canonique D d'un bivecteur est négatif, le bivecteur est dit orienté négativement relativement à la base canonique $\mathcal{B}_0$.
Si le déterminant est nul, les deux vecteurs sont linéairement dépendants.

2° Soit une base $\mathcal{B} = \{u; v\}$.

Si $[\text{Det}\,(u; v)]_{\mathcal{B}_0}$ est positif, la base $\mathcal{B}$ est dite positive ou directe.
Si $[\text{Det}\,(u; v)]_{\mathcal{B}_0}$ est négatif, la base $\mathcal{B}$ est dite négative ou inverse.

La formule (394; 1) montre que l'orientation d'un bivecteur peut être étudiée dans une base positive quelconque.

396. Base canonique de K^3.

Dans l'espace vectoriel K^3, on envisage les vecteurs

$$i = (1;0;0) \qquad j = (0;1;0) \qquad k = (0;0;1).$$

Ces trois vecteurs sont linéairement indépendants; en effet leur déterminant

$$\text{Det}\,(i;j;k) = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} = 1$$

n'est pas nul.

L'ensemble $\mathcal{B}_0 = \{i; j; k\}$ de ces trois vecteurs est appelé la base canonique de l'espace vectoriel K^3.

Remarque.

Dans l'espace vectoriel $\mathcal{M}_1^3$ sur K, la base canonique est l'ensemble des trois vecteurs :

$$i = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \qquad j = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \qquad k = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

397. Expression d'un vecteur dans la base canonique de K^3.

Soit un vecteur quelconque $A = (x; y; z)$ de l'espace vectoriel K^3. On peut écrire :

$$\begin{aligned} A &= (x; y; z) \\ &= (x; 0; 0) + (0; y; 0) + (0; 0; z) \\ &= x \cdot (1; 0; 0) + y \cdot (0; 1; 0) + z \cdot (0; 0; 1) \end{aligned}$$

ou $$A = x \cdot i + y \cdot j + z \cdot k. \qquad (397; 1)$$

Cette expression du vecteur A par une combinaison linéaire des vecteurs de la base $\mathcal{B}_0$ est unique. En effet, soit une seconde décomposition de A :

$$A = x' \cdot i + y' \cdot j + z' \ k \qquad (397; 2)$$

En soustrayant (397; 2) de (397; 1) on obtient :

$$(x - x') \cdot i + (y - y') \cdot j + (z - z') \cdot k = 0$$

Comme les vecteurs i, j, k sont linéairement indépendants les coefficients $x - x'$, $y - y'$, $z - z'$ de cette combinaison linéaire nulle sont tous nuls; d'où :

$$x = x' \qquad y = y' \qquad z = z'$$

On peut alors énoncer :

Un vecteur quelconque de K^3 est une combinaison linéaire unique des vecteurs de la base canonique.

398. Base quelconque de K^3.

Dans l'espace vectoriel K^3, on envisage les vecteurs :

$$u = (\alpha; \beta; \gamma) \qquad v = (\alpha'; \beta'; \gamma') \qquad w = (\alpha''; \beta''; \gamma'')$$

linéairement indépendants, c'est-à-dire que leur déterminant n'est pas nul :

$$D = \text{Det}(u; v; w) = \begin{vmatrix} \alpha & \alpha' & \alpha'' \\ \beta & \beta' & \beta'' \\ \gamma & \gamma' & \gamma'' \end{vmatrix} \neq 0.$$

L'ensemble $\mathcal{B} = \{\mathbf{u}; \mathbf{v}; \mathbf{w};\}$ de ces trois vecteurs linéairement indépendants est une base de l'espace vectoriel K^3.

D'après la formule (397; 1) on a :

$$\begin{cases} u = \alpha \cdot i + \beta \cdot j + \gamma \cdot k \\ v = \alpha' \cdot i + \beta' \cdot j + \gamma' \cdot k \\ w = \alpha'' \cdot i + \beta'' \cdot j + \gamma'' \cdot k \end{cases} \qquad (398; 1)$$

Ces formules donnent les vecteurs u, v, w *de la base $\mathcal{B}$ en fonction des vecteurs* i; j; k *de la base canonique $\mathcal{B}_0$.*

D'autre part, on a :

$$\begin{aligned}
(\beta'\gamma'' - \gamma'\beta'')\, u + (\gamma\beta'' - \beta\gamma'')\, v + (\beta\gamma' - \gamma\beta')\, w
&= (\beta'\gamma'' - \gamma'\beta'')\cdot(\alpha i + \beta' j + \gamma k) \\
&\quad + (\gamma\beta'' - \beta\gamma'')\cdot(\alpha' i + \beta' j + \gamma' k) \\
&\quad + (\beta\gamma' - \gamma\beta')\cdot(\alpha'' i + \beta'' j + \gamma'' k) \\
&= [\alpha(\beta'\gamma'' - \gamma'\beta'') + \alpha'(\gamma\beta'' - \beta\gamma'') + \alpha''(\beta\gamma' - \gamma\beta')]\cdot i \\
&\quad + [\beta(\beta'\gamma'' - \gamma'\beta'') + \beta'(\gamma\beta'' - \beta\gamma'') + \beta''(\beta\gamma' - \gamma\beta')]\cdot j \\
&\quad + [\gamma(\beta'\gamma'' - \gamma'\beta'') + \gamma'(\gamma\beta'' - \beta\gamma'') + \gamma''(\beta\gamma' - \gamma\beta')]\cdot k. \\
&= D\cdot i
\end{aligned}$$

De même :

$$(\gamma'\alpha'' - \alpha'\gamma'')\cdot u + (\alpha\gamma'' - \gamma\alpha'')\, v + (\gamma\alpha' - \alpha\gamma')\, w = D\cdot j$$

et

$$(\alpha'\beta'' - \beta'\alpha'')\cdot u + (\beta\alpha'' - \alpha\beta'')\cdot v + (\alpha\beta' - \beta\alpha')\, w = D\cdot k$$

D'où :

$$\left\{\begin{aligned}
i &= \frac{\begin{vmatrix}\beta' & \gamma' \\ \beta'' & \gamma''\end{vmatrix}}{D}\cdot u + \frac{\begin{vmatrix}\beta'' & \gamma'' \\ \beta & \gamma\end{vmatrix}}{D}\cdot v + \frac{\begin{vmatrix}\beta & \gamma \\ \beta' & \gamma'\end{vmatrix}}{D}\cdot w \\
j &= \frac{\begin{vmatrix}\gamma' & \alpha' \\ \gamma'' & \alpha''\end{vmatrix}}{D}\cdot u + \frac{\begin{vmatrix}\gamma'' & \alpha'' \\ \gamma & \alpha\end{vmatrix}}{D}\cdot v + \frac{\begin{vmatrix}\gamma & \alpha \\ \gamma' & \alpha'\end{vmatrix}}{D}\cdot w \\
k &= \frac{\begin{vmatrix}\alpha' & \beta' \\ \alpha'' & \beta''\end{vmatrix}}{D}\cdot u + \frac{\begin{vmatrix}\alpha'' & \beta'' \\ \alpha & \beta\end{vmatrix}}{D}\cdot v + \frac{\begin{vmatrix}\alpha & \beta \\ \alpha' & \beta'\end{vmatrix}}{D}\cdot w
\end{aligned}\right.$$

Ces formules donnent les vecteurs i; j; k *de la base canonique* $\mathcal{B}_0$ *en fonction des vecteurs* u, v, w *de la base* $\mathcal{B}$.

On pose pour simplifier :

$$\xi = \frac{\begin{vmatrix}\beta' & \gamma' \\ \beta'' & \gamma''\end{vmatrix}}{D} \qquad \eta = \frac{\begin{vmatrix}\beta'' & \gamma'' \\ \beta & \gamma\end{vmatrix}}{D} \qquad \zeta = \frac{\begin{vmatrix}\beta & \gamma \\ \beta' & \gamma'\end{vmatrix}}{D}$$

$$\xi' = \frac{\begin{vmatrix}\gamma' & \alpha' \\ \gamma'' & \alpha''\end{vmatrix}}{D} \qquad \eta' = \frac{\begin{vmatrix}\gamma'' & \alpha'' \\ \gamma & \alpha\end{vmatrix}}{D} \qquad \zeta' = \frac{\begin{vmatrix}\gamma & \alpha \\ \gamma' & \alpha'\end{vmatrix}}{D}$$

$$\xi'' = \frac{\begin{vmatrix}\alpha' & \beta' \\ \alpha'' & \beta''\end{vmatrix}}{D} \qquad \eta'' = \frac{\begin{vmatrix}\alpha'' & \beta'' \\ \alpha & \beta\end{vmatrix}}{D} \qquad \zeta'' = \frac{\begin{vmatrix}\alpha & \beta \\ \alpha' & \beta'\end{vmatrix}}{D}$$

Les formules (398; 2) s'écrivent alors :

$$\left\{\begin{aligned}
i &= \xi\cdot u + \eta\cdot v + \zeta\cdot w \\
j &= \xi'\cdot u + \eta'\cdot v + \zeta'\cdot w \\
k &= \xi''\cdot u + \eta''\cdot v + \zeta''\cdot w
\end{aligned}\right. \qquad (398;\ 3)$$

399. Expression d'un vecteur dans une base quelconque.

Dans l'espace K^3, on considère les deux bases $\mathcal{B}_0 = \{ i; j; k \}$ et $\mathcal{B} = \{ u; v; w \}$.

En remplaçant dans

$$A = x \cdot i + y \cdot j + z \cdot k \qquad (399;1)$$

i, j, k par les formules (398; 3) on obtient :

$$\begin{aligned} A &= x(\xi \cdot u + \eta \cdot v + \zeta \cdot w) + y(\xi' \cdot u + \eta' \cdot v + \zeta' \cdot w) \\ &\qquad + z(\xi'' \cdot u + \eta'' \cdot v + \zeta'' \cdot w) \\ &= (\xi \cdot x + \xi' \cdot y + \xi'' \cdot z)\, u + (\eta \cdot x + \eta' \cdot y + \eta'' \cdot z)\, v \\ &\qquad + (\zeta \cdot x + \zeta' \cdot y + \zeta'' \cdot z) \cdot w \end{aligned}$$

On pose :

$$\begin{cases} X = \xi \cdot x + \xi' \cdot y + \xi'' \cdot z \\ Y = \eta \cdot x + \eta' \cdot y + \eta'' \cdot z \\ Z = \zeta \cdot x + \zeta' \cdot y + \zeta'' \cdot z \end{cases} \qquad (399;2)$$

et

$$A = X \cdot u + Y \cdot v + Z \cdot w. \qquad (399;3)$$

Cette décomposition du vecteur A dans la base $\mathcal{B}$ est unique. En effet soit une seconde décomposition de A :

$$A = X' \cdot u + Y' \cdot v + Z' \cdot w$$

Par soustraction on obtient

$$(X - X') \cdot u + (Y - Y') \cdot v + (Z - Z')\, w = 0$$

Comme les vecteurs u, v et w sont linéairement indépendants, les coefficients $X - X'$, $Y - Y'$ et $Z - Z'$ de cette combinaison linéaire nulle sont nuls; d'où :

$$X = X' \qquad Y = Y' \qquad Z = Z'$$

On peut alors énoncer :

Un vecteur quelconque de K^3 est une combinaison unique des vecteurs d'une base quelconque de K^3.

Les nombres X, Y, Z sont les coordonnées du vecteur a dans la base $\mathcal{B} = \{ u; v; w \}$.

400. Changement de base.

Dans l'espace vectoriel K^3 on considère les bases :

$$\mathcal{B}_0 = \{ i; j; k \} \quad \text{et} \quad \mathcal{B} = \{ u; v; w \}$$

la base $\mathcal{B}_0$ n'étant plus nécessairement la base canonique.

On donne :

$$\begin{cases} u = \alpha \cdot i + \beta \cdot j + \gamma \cdot k \\ v = \alpha' \cdot i + \beta' \cdot j + \gamma' \cdot k \\ w = \alpha'' \cdot i + \beta'' \cdot j + \gamma'' \cdot k \end{cases} \qquad (400;1)$$

Comme au nº 398, on en déduit :

$$\begin{cases} i = \xi \cdot u + \eta \cdot v + \zeta \cdot w \\ j = \xi' \cdot u + \eta' \cdot v + \zeta' \cdot w \\ k = \xi'' \cdot u + \eta'' \cdot v + \zeta'' \cdot w \end{cases} \qquad (400;2)$$

Dans la base $\mathcal{B}_0$, on a :

$$A = x \cdot i + y \cdot j + z \cdot k \qquad (400;3)$$

et dans la base $\mathcal{B}$:

$$A = X \cdot u + Y \cdot v + Z \cdot w \qquad (400;4)$$

1º Le calcul du nº 399, donne

$$\begin{cases} X = \xi \cdot x + \xi' \cdot y + \xi'' \cdot z \\ Y = \eta \cdot x + \eta' \cdot y + \eta'' \cdot z \\ Z = \zeta \cdot x + \zeta' \cdot y + \zeta'' \cdot z \end{cases} \qquad (400;5)$$

Ces formules donnent les coordonnées X, Y, Z du vecteur A dans la base $\mathcal{B}$ en fonction des coordonnées x, y, z du même vecteur A dans la base $\mathcal{B}_0$.

2º En remplaçant dans $A = X \cdot u + Y \cdot v + Z \cdot w$, u, v, w par les expressions (400; 1), on obtient :

$$\begin{aligned} A &= X(\alpha \cdot i + \beta \cdot j + \gamma \cdot k) + Y(\alpha' \cdot i + \beta' \cdot j + \gamma' \cdot k) \\ &\qquad + Z(\alpha'' \cdot i + \beta'' \cdot j + \gamma'' \cdot k) \\ &= (\alpha \cdot X + \alpha' \cdot Y + \alpha'' \cdot Z) \cdot i + (\beta \cdot X + \beta' \cdot Y + \beta'' \cdot Z) \cdot j \\ &\qquad + (\gamma \cdot X + \gamma' \cdot Y + \gamma'' \cdot Z) \cdot k. \end{aligned}$$

En comparant à (400; 3), et par suite de l'unicité de la décomposition du vecteur A dans $\mathcal{B}_0$, on déduit :

$$\begin{cases} x = \alpha \cdot X + \alpha' \cdot Y + \alpha'' \cdot Z \\ y = \beta \cdot X + \beta' \cdot Y + \beta'' \cdot Z \\ z = \gamma \cdot X + \gamma' \cdot Y + \gamma'' \cdot Z \end{cases} \qquad (400;6)$$

Ces formules donnent les coordonnées x, y, z du vecteur A dans la base $\mathcal{B}_0$ en fonction des coordonnées X, Y, Z du même vecteur A dans la base $\mathcal{B}$.

Les formules (400; 5) et (400; 6) sont les *formules de changement de base dans* K^3.

401. Addition des vecteurs et changement de base dans K^3.

Soient les vecteurs :

$$A = (x; y; z) \qquad B = (x'; y'; z')$$

et leur somme $S = A + B = (x + x'; y + y'; z + z')$

Ces trois vecteurs sont donnés dans la base $\mathcal{B}_0$.

Dans la base $\mathcal{B} = \{u; v\}$ les coordonnées de A et B sont X, Y, Z et X', Y', Z' respectivement, avec :

$$\begin{cases} X = \xi \cdot x + \xi' \cdot y + \xi'' \cdot z \\ Y = \eta \cdot x + \eta' \cdot y + \eta'' \cdot z \\ Z = \zeta \cdot x + \zeta' \cdot y + \zeta'' \cdot z \end{cases} \qquad \begin{cases} X' = \xi \cdot x' + \xi' \cdot y' + \xi'' \cdot z' \\ Y' = \eta \cdot x' + \eta' \cdot y' + \eta'' \cdot z' \\ Z' = \zeta \cdot x' + \zeta' \cdot y' + \zeta'' \cdot z' \end{cases}$$

Les coordonnées X'', Y'', Z'' dans $\mathcal{B}$ de la somme $S = A + B$ sont données par les formules (400; 5) :

$$\begin{cases} X'' = \xi\,(x + x') + \xi'\,(y + y') + \xi''\,(z + z') \\ \quad = (\xi x + \xi' y + \xi'' z) + (\xi x' + \xi' y' + \xi'' z') \\ \quad = X + X' \\ Y'' = \eta\,(x + x') + \eta'\,(y + y') + \eta''(z + z') \\ \quad = (\eta x + \eta' y + \eta'' z) + (\eta x' + \eta' y' + \eta'' z') \\ \quad = Y + Y' \\ Z'' = \zeta\,(x + x') + \zeta'\,(y + y') + \zeta''\,(z + z') \\ \quad = (\zeta x + \zeta' y + \zeta'' z) + (\zeta x' + \zeta' y' + \zeta'' z') \\ \quad = Z + Z' \end{cases}$$

Donc la somme $S = A + B$ se calcule de la même façon dans la base $\mathcal{B}$ et dans la base $\mathcal{B}_0$

Et :

L'addition des vecteurs est intrinsèque.

402. Produit d'un vecteur par un nombre et changement de base.

Soient le vecteur $A = (x; y; z)$ et le scalaire λ. On considère le produit $\lambda \cdot A$:
$$P = \lambda \cdot A = (\lambda x; \lambda y; \lambda z).$$

Ces vecteurs A et P sont donnés dans la base $\mathcal{B}_0$.

Dans la base $\mathcal{B} = \{u; v; w\}$ les coordonnées de A sont X, Y, Z, avec

$$\begin{cases} X = \xi x + \xi' y + \xi'' z \\ Y = \eta x + \eta' y + \eta'' z \\ Z = \zeta x + \zeta' y + \zeta'' z \end{cases}$$

Les coordonnées X'', Y'', Z'' dans $\mathcal{B}$ du vecteur $P = \lambda A$ sont données par les formules (400; 5) :

$$\begin{cases} X'' = \xi \cdot (\lambda x) + \xi' \cdot (\lambda y) + \xi'' \cdot (\lambda z) = \lambda\,(\xi x + \xi' y + \xi'' z) = \lambda \cdot X \\ Y'' = \eta \cdot (\lambda x) + \eta' \cdot (\lambda y) + \eta'' \cdot (\lambda z) = \lambda\,(\eta x + \eta' y + \eta'' z) = \lambda \cdot Y \\ Z'' = \zeta \cdot (\lambda x) + \zeta' \cdot (\lambda y) + \zeta'' \cdot (\lambda z) = \lambda\,(\zeta x + \zeta' y + \zeta'' z) = \lambda \cdot Z \end{cases}$$

Donc le produit $P = \lambda A$ se calcule de la même façon dans la base $\mathcal{B}$ et dans la base $\mathcal{B}_0$.

Et :

La multiplication d'un vecteur par un scalaire est intrinsèque.

403. Remarque.

L'addition des vecteurs et la multiplication d'un vecteur par un scalaire étant intrinsèques, on déduit

La dépendance linéaire et l'indépendance linéaire de plusieurs vecteurs sont intrinsèques.

404. Déterminant et changement de base.

Soient les vecteurs A, B, et C.

Dans la base $\mathcal{B}_0 = \{ i; j; k \}$ on a :

$$\begin{cases} A = x \cdot i + y \cdot j + z \cdot k \\ B = x' \cdot i + y' \cdot j + z' \cdot k \\ C = x'' \cdot i + y'' \cdot j + z'' \cdot k \end{cases}$$

et dans la base $\mathcal{B} = \{ u; v; w \}$:

$$\begin{cases} A = X \cdot u + Y \cdot v + Z \cdot w \\ B = X' \cdot u + Y' \cdot v + Z' \cdot w \\ C = X'' \cdot u + Y'' \cdot v + Z'' \cdot w \end{cases}$$

On note :

$$[\mathrm{Det}\,(A; B; C)]_{\mathcal{B}_0} = \begin{vmatrix} x & x' & x'' \\ y & y' & y'' \\ z & z' & z'' \end{vmatrix}$$

et

$$[\mathrm{Det}\,(A; B; C)]_{\mathcal{B}_0} = \begin{vmatrix} X & X' & X'' \\ Y & Y' & Y'' \\ Z & Z' & Z'' \end{vmatrix}$$

On a :

$$\begin{aligned} [\mathrm{Det}\,(A; B; C)]_{\mathcal{B}_0} &= [\mathrm{Det}\,(Xu + Yv + Zw; B; C)]_{\mathcal{B}_0} \\ &= X \cdot [\mathrm{Det}\,(u; B; C)]_{\mathcal{B}_0} + Y \cdot \mathrm{Det}\,(v; B; C)]_{\mathcal{B}_0} \\ &\qquad + Z \cdot [\mathrm{Det}\,(w; B; C)]_{\mathcal{B}_0} \end{aligned}$$

Or :

$$\begin{aligned} [\mathrm{Det}\,(u; B; C)]_{\mathcal{B}_0} &= [\mathrm{Det}\,(u; X'u + Y'v + Z'w; C)]_{\mathcal{B}_0} \\ &= [\mathrm{Det}\,(u; X'u; C)]_{\mathcal{B}_0} + [\mathrm{Det}\,(u; Y'v; C)]_{\mathcal{B}_0} \\ &\qquad + [\mathrm{Det}\,(u; Z'w; C)]_{\mathcal{B}_0} \\ &= [\mathrm{Det}\,(u; Y'v; C)]_{\mathcal{B}_0} + [\mathrm{Det}\,(u; Z'w; C)]_{\mathcal{B}_0} \\ &= Y' \cdot [\mathrm{Det}\,(u; v; C)]_{\mathcal{B}_0} + Z' \cdot [\mathrm{Det}\,(u; w; C)]_{\mathcal{B}_0} \end{aligned}$$

avec

$$\begin{aligned}[\mathrm{Det}\,(u;\,v;\,C)]_{\mathcal{B}_0} &= [\mathrm{Det}\,(u;\,v;\,X''u + Y''v + Z''w)]_{\mathcal{B}_0} \\ &= [\mathrm{Det}\,(u;\,v;\,X''u)]_{\mathcal{B}_0} + [\mathrm{Det}\,(u;\,v;\,Y''v)]_{\mathcal{B}_0} \\ &\qquad\qquad + \mathrm{Det}\,(u;\,v;\,Z''w]_{\mathcal{B}_0} \\ &= [\mathrm{Det}\,(u;\,v;\,Z''w)]_{\mathcal{B}_0} \\ &= Z''\ [\mathrm{Det}\,(u;\,v;\,w)]_{\mathcal{B}_0}\end{aligned}$$

et

$$\begin{aligned}[\mathrm{Det}\,(u;\,w;\,C)]_{\mathcal{B}_0} &= [\mathrm{Det}\,(u;\,w;\,X''u + Y''v + Z''w)]_{\mathcal{B}_0} \\ &= [\mathrm{Det}\,(u;\,w;\,Y''v)]_{\mathcal{B}_0} \\ &= Y''\cdot[\mathrm{Det}\,(u;\,w;\,v)]_{\mathcal{B}_0} \\ &= -\,Y''\cdot[\mathrm{Det}\,(u;\,v;\,w)]_{\mathcal{B}_0}\end{aligned}$$

D'où :

$$\begin{aligned}[\mathrm{Det}\,(u;\,B;\,C)]_{\mathcal{B}_0} &= Y'Z''\cdot[\mathrm{Det}\,(u;\,v;\,w)]_{\mathcal{B}_0} - Z'Y''\cdot[\mathrm{Det}\,u;\,v;\,w]_{\mathcal{B}_0} \\ &= (Y'Z'' - Z'Y'')\cdot[\mathrm{Det}\,(u;\,v;\,w)]_{\mathcal{B}_0}\end{aligned}$$

De même :

$$[\mathrm{Det}\,(v;\,B;\,C)]_{\mathcal{B}_0} = (Z'X'' - X'Z'')\cdot[\mathrm{Det}\,(u;\,v;\,w)]_{\mathcal{B}_0}$$

et

$$[\mathrm{Det}\,(w;\,B;\,C)]_{\mathcal{B}_0} = (X'Y'' - Y'X'')\cdot[(\mathrm{Det}\,(u;\,v;\,w)]_{\mathcal{B}_0}$$

En remplaçant dans (404; 1) on obtient :

$$\begin{aligned}[\mathrm{Det}\,(A;\,B;\,C)]_{\mathcal{B}_0} = [X\,(Y'Z'' - Z'Y'') &+ Y\,(Z'X'' - X'Z'') \\ &+ Z\,(X'Y'' - Y'X'')]\cdot[\mathrm{Det}\,(u;\,v;\,w)]_{\mathcal{B}_0}\end{aligned}$$

D'où la formule :

$$[\mathbf{Det}\,(A;\,B;\,C)]_{\mathcal{B}_0} = [\mathbf{Det}\,(u;\,v;\,w)]_{\mathcal{B}_0} \times [\mathbf{Det}\,(A;\,B;\,C)]_{\mathcal{B}} \quad (404;\,2)$$

Le déterminant n'est donc pas intrinsèque.

405. Orientation d'un trivecteur de R^3.

On envisage dans ce numéro l'espace vectoriel R^3 rapporté à sa base canonique $\mathcal{B}_0$.

1° Soient le trivecteur (A; B; C) de l'espace vectoriel R^3. Le déterminant de ce trivecteur dans la base $\mathcal{B}_0$ est $D = \mathrm{Det}\,(A;\,B;\,C)$.

Si le déterminant canonique D d'un trivecteur est positif, le trivecteur est dit orienté positivement relativement à la base canonique $\mathcal{B}_0$.

Si le déterminant canonique D d'un trivecteur est négatif, le trivecteur est dit orienté négativement relativement à la base canonique $\mathcal{B}_0$.

Si le déterminant est nul, les trois vecteurs sont linéairement dépendants.

2° Soit une base $\mathcal{B} = \{ u; v; w \}$.

Si Det $(u; v; w)$ *est positif, la base* $\mathcal{B}$ *est dite positive ou directe.*

Si Det $(u; v; w)$ *est négatif, la base* $\mathcal{B}$ *est dite négative ou inverse.*

La formule (404; 2) montre que l'orientation d'un trivecteur peut être étudiée dans une base positive quelconque.

406. Variétés linéaires.

1° ***Soit un vecteur A de*** K^2 ***ou de*** K^3. ***On considère l'ensemble F de tous les vecteurs*** $U = \lambda A$, λ ***étant un scalaire quelconque du corps K :***

$$F = \{ U/U = \lambda \cdot A \quad \text{et} \quad \lambda \in K \}.$$

Cet ensemble F de vecteurs est une variété linéaire de dimension 1, car tous les vecteurs de F s'expriment à l'aide du seul vecteur A. On dit aussi que F est un sous-espace vectoriel de dimension 1.

◇ *Exemple 1.*

Soit l'espace vectoriel K^2 *avec* $K = Z/5$. *On considère le vecteur* $A = (\dot{2}; \dot{3})$. *Trouver la variété linéaire engendrée par le vecteur A.*

$F = \{ U_0; U_1; U_2; U_3; U_4 \}$ avec :

$$U_0 = \dot{0} \cdot A = (\dot{0}; \dot{0})$$
$$U_1 = \dot{1} \cdot A = (\dot{2}; \dot{3})$$
$$U_2 = \dot{2} \cdot A = (\dot{4}; \dot{1})$$
$$U_3 = \dot{3} \cdot A = (\dot{1}; \dot{4})$$
$$U_4 = \dot{4} \cdot A = (\dot{3}; \dot{2})$$

2° ***Soient deux vecteurs A et B, non nuls et linéairement indépendants.***

On considère l'ensemble F de tous les vecteurs $U = \lambda \cdot A + \mu \cdot B$, λ ***et*** μ ***étant des scalaires quelconques du corps K :***

$$F = \{ U/U = \lambda \cdot A + \mu \cdot B, \lambda \in K, \mu \in K \}.$$

Cet ensemble F de vecteurs est une variété linéaire, de dimension 2, car tous les vecteurs de F s'expriment à l'aide des deux vecteurs A et B. On dit aussi que F est un sous-espace vectoriel de dimension 2.

◇ *Exemple 2.*

Soit l'espace vectoriel K^3 *avec* $K = Z/3$. *On considère les vecteurs* $A = (\dot{1}; \dot{2}; \dot{1})$ *et* $B = (\dot{1}; \dot{1}; \dot{2})$. *Etudier la variété linéaire engendrée par les vecteurs A et B.*

$F = \{ U/U = \lambda \cdot A + \mu \cdot B \}$ est formé des 9 vecteurs suivants :

$$\begin{array}{lll}
\lambda = \dot{0} & \mu = \dot{0} & U = (\dot{0}; \dot{0}; \dot{0}) \\
\lambda = \dot{0} & \mu = \dot{1} & U = (\dot{1}; \dot{1}; \dot{2}) \\
\lambda = \dot{0} & \mu = \dot{2} & U = (\dot{2}; \dot{2}; \dot{1}) \\
\lambda = \dot{1} & \mu = \dot{0} & U = (\dot{1}; \dot{2}; \dot{1}) \\
\lambda = \dot{1} & \mu = \dot{1} & U = (\dot{2}; \dot{0}; \dot{0}) \\
\lambda = \dot{1} & \mu = \dot{2} & U = (\dot{0}; \dot{1}; \dot{2}) \\
\lambda = \dot{2} & \mu = \dot{0} & U = (\dot{2}; \dot{1}; \dot{2}) \\
\lambda = \dot{2} & \mu = \dot{1} & U = (\dot{0}; \dot{2}; \dot{1}) \\
\lambda = \dot{2} & \mu = \dot{2} & U = (\dot{1}; \dot{0}; \dot{0})
\end{array}$$

◇ *Exemple 3.*

Dans R^3 on considère les vecteurs $A = (1; -1; 2)$ et $B = (2; 1; -2)$. Etudier la variété linéaire engendrée par A et B.

$$F = \{U/U = \lambda \cdot A + \mu \cdot B, \lambda \in R \text{ et } \mu \in R\}$$

Ici on ne peut donner tous les vecteurs. Mais il est possible de donner U par ses coordonnées :

$$\begin{aligned}
X &= \lambda \cdot (1) + \mu \cdot (2) \\
Y &= \lambda \cdot (-1) + \mu \cdot (1) \\
Z &= \lambda \cdot (2) + \mu \cdot (-2)
\end{aligned}$$

ou

$$\begin{cases}
X = \lambda + 2\mu \\
Y = -\lambda + \mu \\
Z = 2\lambda - 2\mu
\end{cases}$$

CHAPITRE XXXII

ESPACES VECTORIELS EUCLIDIENS

407. Produit scalaire euclidien.

Soit l'espace vectoriel $E = R^3$, rapporté à la base canonique $\mathcal{B}_0 = \{i; j; k;\}$.

On considère deux vecteurs de cet espace euclidien :

$$V = (x; y; z) \quad \text{et} \quad V' = (x'; y'; z')$$

On appelle produit scalaire euclidien relativement à la base $\mathcal{B}_0$ l'application S définie par :

$$S : \quad (V; V') \in E^2 \longrightarrow S(V; V') = xx' + yy' + zz'$$

On note :

$$V \cdot V' = xx' + yy' + zz' \qquad (407; 1)$$

et on lit « V scalaire V' ».

Par abus du langage, le nombre $xx' + yy' + zz'$ est aussi appelé le produit scalaire des deux vecteurs.

Remarque.

Dans l'espace vectoriel R^2, on a évidemment

$$V \cdot V' = xx' + yy' \qquad (407; 2)$$

et dans l'espace vectoriel R :

$$V \cdot V' = xx'. \qquad (407; 3)$$

408. Propriétés du produit scalaire.

Le produit scalaire possède les propriétés suivantes :

1° Commutativité.

On a :

$$V \cdot V' = xx' + yy' + zz'$$

et

$$V' \cdot V = x'x + y'y + z'z$$

Les deux résultats sont identiques. Donc :

$$(\forall V)(\forall V') \quad V \cdot V' = V' \cdot V \qquad (408;1)$$

et :

La multiplication scalaire euclidienne de deux vecteurs de R^3 est commutative.

2° **Distributivité.**

On a :

$$\begin{aligned}(V_1 + V_2) \cdot V' &= (x_1 + x_2)\, x' + (y_1 + y_2)\, y' + (z_1 + z_2)\, z' \\ &= (x_1x' + y_1y' + z_1z') + (x_2x' + y_2y' + z_2z')\end{aligned}$$

et

$$V_1 \cdot V' + V_2 \cdot V' = (x_1x' + y_1y' + z_1z') + (x_2x' + y_2y' + z_2z')$$

Les deux résultats sont identiques; donc

$$(\forall V_1)(\forall V_2)(\forall V') \quad (V_1 + V_2) \cdot V' = V_1 \cdot V' + V_2 \cdot V' \qquad (408;2)$$

De même :

$$(\forall V)(\forall V'_1)(\forall V'_2) \quad V \cdot (V'_1 + V'_2) = V \cdot V'_1 + V \cdot V'_2 \qquad (408;3)$$

Et :

La multiplication scalaire euclidienne de deux vecteurs de R^3 est distributive pour l'addition des vecteurs.

3° **Associativité mixte.**

On a :

$$\begin{aligned}(\lambda V) \cdot V' &= (\lambda x)\, x' + (\lambda y)\, y' + (\lambda z)\, z' \\ &= \lambda\, (xx' + yy' + zz')\end{aligned}$$

et

$$\lambda \cdot (V \cdot V') = \lambda\, (xx' + yy' + zz').$$

Les deux résultats sont identiques; donc

$$(\forall \lambda)(\forall V)(\forall V') : \quad (\lambda V) \cdot V' \cdot = \lambda \,.\, (V \cdot V') \qquad (408;4)$$

En tenant compte de la commutativité :

$$V \cdot (\lambda V') = \lambda \cdot (V \cdot V') \qquad (408;5)$$

Et :

La multiplication scalaire euclidienne de deux vecteurs de R^3 est associative avec la multiplication par un nombre réel.

4° On a :

$$V \cdot V = x^2 + y^2 + z^2$$

ou

$$\mathbf{V}^2 = \mathbf{x}^2 + \mathbf{y}^2 + \mathbf{z}^2. \qquad (408;6)$$

409. Remarque.

Les propriétés précédentes permettent d'établir les formules suivantes :

1°
$$\begin{aligned}(U + V)^2 &= (U + V)\cdot(U + V)\\ &= U\cdot(U + V) + V\cdot(U + V)\\ &= U^2 + U\cdot V + V\cdot U + V^2\end{aligned}$$

ou
$$(U + V)^2 = U^2 + 2\,U\cdot V + V^2 \qquad (409;\ 1)$$

2° De même
$$(U - V)^2 = U^2 - 2\,U\cdot V + V^2. \qquad (409;\ 2)$$

3° On a :
$$\begin{aligned}(U + V)\cdot(U - V) &= U\,(U - V) + V\,(U - V)\\ &= U^2 - U\cdot V + V\cdot U - V^2\end{aligned}$$

ou
$$(U + V)\cdot(U - V) = U^2 - V^2. \qquad (409;\ 3)$$

410. Norme euclidienne d'un vecteur.

Soit un vecteur de R^3 : $V = (x;\ y;\ z)$. R^3 est rapporté à sa base canonique.

On appelle norme euclidienne du vecteur V, associée au produit scalaire euclidien, l'application N définie par

$$N :\qquad V \in E \longrightarrow N(V) = \sqrt{V\cdot V} \in R_+.$$

Donc :
$$\begin{aligned}N(V) &= \sqrt{V^2}\\ &= \sqrt{x^2 + y^2 + z^2}\end{aligned} \qquad (410;\ 1)$$

On note aussi très souvent :
$$N(V) = \|V\| = \sqrt{x^2 + y^2 + z^2} \qquad (410;\ 2)$$

et on a :
$$V^2 = \|V\|^2. \qquad (410;\ 3)$$

Par abus de langage, le nombre positif $\sqrt{x^2 + y^2 + z^2}$ est aussi appelé la norme euclidienne du vecteur, relativement à la base canonique $\mathcal{B}_0$.

Remarque.

Dans l'espace vectoriel R^2, on a évidemment :
$$\|V\| = \sqrt{x^2 + y^2} \qquad (410;\ 4)$$

et dans l'espace vectoriel R :
$$\|V\| = |x| \qquad (410;\ 5)$$

411. Inégalité de Schwarz.

Soient deux vecteurs U et V.

Quel que soit le nombre $\lambda \in R$, on a :

$$0 \leqslant (\lambda U + V)^2 = \lambda^2 U^2 + 2\lambda U \cdot V + V^2$$
$$= \lambda^2 \cdot \| U \|^2 + 2\lambda \cdot U \cdot V + \| V \|^2. \quad (411;1)$$

Si $U \cdot V \neq 0$ en posant $\lambda = -\dfrac{\| V \|^2}{U \cdot V}$ et un remplaçant dans (411; 1), on obtient :

$$0 \leqslant \frac{\| V \|^4}{(U \cdot V)^2} \cdot \| U \|^2 - 2 \frac{\| V \|^2}{(U \cdot V)} \cdot (U \cdot V) + \| V \|^2$$

ou

$$0 \leqslant \frac{\| V \|^4}{(U \cdot V)^2} \| U \|^2 - \| V \|^2$$

ou, en divisant par $\| V \|^2$:

$$0 \leqslant \frac{\| U \|^2 \cdot \| V \|^2}{(U \cdot V)^2} - 1$$

et enfin :

$$| U \cdot V | \leqslant \| U \| \cdot \| V \|.$$

Si $U \cdot V = 0$, on a évidemment :

$$0 \leqslant \| U \| \cdot \| V \|$$

ou

$$| U \cdot V | \leqslant \| U \| \cdot \| V \|.$$

Dans les deux cas, on a donc :

$$| \boldsymbol{U} \cdot \boldsymbol{V} | \leqslant \| \boldsymbol{U} \| \cdot \| \boldsymbol{V} \| \quad (411;2)$$

C'est l'inégalité de Schwarz.

412. Propriétés de la norme euclidienne.

La norme euclidienne possède les propriétés suivantes.

1° Quel que soit le vecteur $V = (x; y; z)$ on a $\| V \| = \sqrt{x^2 + y^2 + z^2}$. On en déduit :

N₁ $$(\| V \| = 0) \quad \Leftrightarrow \quad (V = 0) \quad (412;1)$$

2° On a

$$\| \lambda \cdot V \| = \sqrt{(\lambda x)^2 + (\lambda y)^2 + (\lambda z)^2}$$
$$= \sqrt{\lambda^2 (x^2 + y^2 + z^2)}$$
$$= | \lambda | \cdot \sqrt{x^2 + y^2 + z^2}.$$

Donc :

N₂ $(\forall\lambda)(\forall V): \quad \|\lambda V\| = |\lambda| \cdot \|V\|$ (412; 2)

3° On a :

$$(U + V)^2 = U^2 + 2 \cdot U \cdot V + V^2$$
$$= \|U\|^2 + 2 \cdot U \cdot V + \|V\|^2.$$

Or :

$$U \cdot V \leqslant |U \cdot V|$$

et (inégalité de Schwarz) :

$$|U \cdot V| \leqslant \|U\| \cdot \|V\|.$$

Donc :

$$U \cdot V \leqslant \|U\| \cdot \|V\|.$$

Par suite :

$$(U + V)^2 \leqslant \|U\|^2 + 2 \cdot \|U\| \cdot \|V\| + \|V\|^2$$

ou

$$\|U + V\|^2 \leqslant (\|U\| + \|V\|)^2$$

Et :

N₃ $(\forall U)(\forall V): \quad \|U + V\| \leqslant \|U\| + \|V\|$ (412; 3)

413. Vecteurs unitaires.

1° ***Un vecteur $V = (x; y; z)$ est dit vecteur unitaire (ou vecteur normé) si sa norme est l'unité, c'est-à-dire si $\|V\| = 1$ ou***

$$x^2 + y^2 + z^2 = 1.$$

2° Soient les vecteurs de la base canonique $\mathcal{B}_0 = \{ i; j; k \}$:

$$i = (1; 0; 0) \qquad j = (0; 1; 0) \qquad k = (0; 0; 1)$$

On a :

$$\|i\| = 1 \qquad \|j\| = 1 \qquad \|k\| = 1.$$

Donc :

Les vecteurs de la base canonique de l'espace euclidien R^3 sont unitaires.

◇ *Exemple.*

Soit dans R^3, le vecteur $u = \left(\frac{2}{3}; -\frac{2}{3}; \frac{1}{3}\right)$. Calculer sa norme.

On a :

$$\|u\|^2 = \frac{4}{9} + \frac{4}{9} + \frac{1}{9} = 1$$

Donc :

$$\|u\| = 1.$$

et le vecteur u est un vecteur unitaire.

414. Vecteurs orthogonaux.

1° Soient deux vecteurs $V = (x; y; z)$ et $V' = (x'; y'; z')$.

Les deux vecteurs V et V', non nuls, sont dits orthogonaux si leur produit scalaire euclidien est nul;

c'est-à-dire si on a :

$$V \cdot V' = xx' + yy' + zz' = 0$$

On note :

$$V \perp V'$$

et on lit « V orthogonal à V' ».

Donc :

$$\mathbf{(V \perp V') \iff (xx' + yy' + zz' = 0).} \qquad (414; 1)$$

2° Soient dans R^2, les vecteurs de la base canonique $\mathcal{B}_0$:

$$i = (1; 0) \qquad \text{et} \qquad j = (0; 1).$$

On a :

$$\begin{aligned} i \cdot j &= 1 \times 0 + 0 \times 1 \\ &= 0 \end{aligned}$$

Donc :

$$i \perp j.$$

Et :

Les vecteurs de la base canonique de R^2 sont orthogonaux.

3° De même dans R^3, soient les vecteurs de la base canonique $\mathcal{B}_0$:

$$i = (1; 0; 0) \qquad j = (0; 1; 0) \qquad k = (0; 0; 1)$$

On a :

$$i \cdot j = 0 \qquad i \cdot k = 0 \qquad j \cdot k = 0$$

ou

$$i \perp j \qquad i \perp k \qquad j \perp k$$

Et :

Les vecteurs de la base canonique de R^3 sont orthogonaux deux à deux.

◇ *Exemple.*

Dans R^3, on donne les vecteurs $V = (2; 2; 1)$ et $(V' = -3; 2; 2)$. Montrer que ces vecteurs sont orthogonaux.

En effet on a :

$$\begin{aligned} V \cdot V' &= -6 + 4 + 2 \\ &= 0 \end{aligned}$$

Donc :

$$V \perp V'.$$

415. Bases orthonormées.

1° Base orthonormée dans $\mathbf{R}^2$.

Une base $\mathcal{B} = \{u; v\}$ de l'espace vectoriel est orthonormée si les vecteurs u et v sont unitaires et orthogonaux;

c'est-à-dire si

$$\|u\| = 1, \quad \|v\| = 1 \quad \text{et} \quad u \perp v$$

ou

$$\|u\| = 1, \quad \|v\| = 1 \quad \text{et} \quad u \cdot v = 0.$$

La base canonique $\mathcal{B}_0 = \{i; j\}$ de $\mathbf{R}^2$ est orthonormée,

car :

$$\|i\| = 1, \quad \|j\| = 1 \text{ et } \quad i \perp j$$

◇ *Exemples.*

Dans R^2, on considère les vecteurs $u = \left(\frac{2}{\sqrt{5}}; -\frac{1}{\sqrt{5}}\right)$ et $v = \left(\frac{1}{\sqrt{5}}; \frac{2}{\sqrt{5}}\right)$.
Montrer qu'ils forment une base orthonormée.

On a:

$$\text{Det}(u; v) = \begin{vmatrix} \frac{2}{\sqrt{5}} & \frac{1}{\sqrt{5}} \\ -\frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} \end{vmatrix} = \frac{4}{5} + \frac{1}{5} = 1.$$

Les vecteurs u et v sont donc linéairement indépendants; ils forment une base $\mathcal{B} = \{u; v\}$.

On a encore :

$$\|u\| = \sqrt{\frac{4}{5} + \frac{1}{5}} = 1$$

$$\|v\| = \sqrt{\frac{1}{5} + \frac{4}{5}} = 1$$

et

$$u \cdot v = \frac{2}{5} - \frac{2}{5} = 0.$$

Donc la base $\mathcal{B}$ est orthonormée.

2° Base orthonormée de $\mathbf{R}^3$.

Une base $\mathcal{B} = \{u; v; w;\}$ de l'espace vectoriel R^3 est orthonormée si les vecteurs u, v, w sont unitaires et deux à deux orthogonaux;

c'est-à-dire si

$$\|u\| = 1 \quad \|v\| = 1 \quad \|w\| = 1 \quad u \perp v \quad u \perp w \quad v \perp w$$

ou

$$\|u\| = 1 \quad \|v\| = 1 \quad \|w\| = 1 \quad u \cdot v = 0 \quad u \cdot w = 0 \quad v \cdot w = 0.$$

La base canonique $\mathcal{B}_0 = \{i; j; k\}$ de R^3 est orthonormée

car :

$$\|i\| = 1 \quad \|j\| = 1 \quad \|k\| = 1 \quad i \perp j \quad i \perp k \quad j \perp k.$$

◇ *Exemple.*

Dans R^3 on considère les vecteurs $u = \left(\frac{2}{3}; \frac{2}{3}; \frac{1}{3}\right)$, $v = \left(\frac{2}{3}; \frac{1}{3}; \frac{2}{3}\right)$ $w = \left(\frac{1}{3}; -\frac{2}{3}; \frac{2}{3}\right)$. *Montrer qu'ils forment une base orthonormée.*

$\mathcal{B} = \{ u ; v ; w \}$ est une base, car :

$$\text{Det}\,(u ; v ; w) = \begin{vmatrix} \frac{2}{3} & -\frac{2}{3} & \frac{1}{3} \\ \frac{2}{3} & \frac{1}{3} & -\frac{2}{3} \\ \frac{1}{3} & \frac{2}{3} & \frac{2}{3} \end{vmatrix}$$

$$= \frac{4}{27} + \frac{4}{27} + \frac{4}{27} - \frac{1}{27} + \frac{8}{27} + \frac{8}{27}$$

n'est pas nul. $= 1$

De plus :

$$\|u\| = \sqrt{\frac{4}{9} + \frac{4}{9} + \frac{1}{9}} = 1$$

$$\|v\| = \sqrt{\frac{4}{9} + \frac{1}{9} + \frac{4}{9}} = 1$$

$$\|w\| = \sqrt{\frac{1}{9} + \frac{4}{9} + \frac{4}{9}} = 1$$

et

$$u \cdot v = \left(\frac{2}{3}\right)\left(-\frac{2}{3}\right) + \left(\frac{2}{3}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{3}\right) \cdot \left(\frac{2}{3}\right) = 0$$

$$u \cdot w = \left(\frac{2}{3}\right)\left(\frac{1}{3}\right) + \left(\frac{2}{3}\right)\left(-\frac{2}{3}\right) + \left(\frac{1}{3}\right)\left(\frac{2}{3}\right) = 0$$

$$v \cdot w = \left(-\frac{2}{3}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{3}\right)\left(-\frac{2}{3}\right) + \left(\frac{2}{3}\right)\left(\frac{2}{3}\right) = 0.$$

La base $\mathcal{B}$ est donc orthonormée.

416. Variétés orthogonales.

1° ***Deux variétés linéaires F et F′ sont dites orthogonales si tout vecteur de F est orthogonal à tous les vecteurs de F′.***

On note :

$$F \perp F'$$

Donc :

$$(F \perp F') \Leftrightarrow (\forall V)(V \in F); (\forall V')(V' \in F') : \quad V \perp V'$$

ou

$$(F \perp F') \Leftrightarrow (\forall V)(V \in F); (\forall V')(V' \in F') : \quad V \cdot V' = 0.$$

2° *Condition d'orthogonalité de deux variétés de dimension 1.*

Soient dans R^2 (ou dans R^3) deux variétés linéaires F et F′ de dimension 1.

F est déterminée par un vecteur A, et on a :

$$F = \{ U/U = \lambda \cdot A, \lambda \in R \}.$$

F′ est déterminée par un vecteur B, et on a :

$$F' = \{ V/V = \mu \cdot B, \mu \in R \}$$

On a :

$$\begin{aligned} U \cdot V &= (\lambda \cdot A) \cdot (\mu \cdot B) \\ &= (\lambda\mu) \cdot (A \cdot B) \end{aligned}$$

Or :

$$\begin{aligned} (F \perp F') &\Leftrightarrow (\forall \lambda)(\forall \mu) \quad U \cdot V = 0 \\ &\Leftrightarrow A \cdot B = 0 \\ &\Leftrightarrow A \perp B. \end{aligned}$$

Et :

Pour que deux variétés linéaires F et F′, de dimension 1, soient orthogonales il faut et il suffit qu'un vecteur A de F soit orthogonal à un vecteur B de F′.

3° *Condition d'orthogonalité d'une variété de dimension 1 et d'une variété de dimension 2.*

Soient dans R^3 une variété linéaire de dimension 1, déterminée par le vecteur A :

$$F = \{U/U = \rho \cdot A, \rho \in R\}$$

et une variété linéaire de dimension 2, déterminée par les vecteurs B et C linéairement indépendants :

$$F' = \{ V/V = \lambda \cdot B + \mu \cdot C, \lambda \in R, \mu \in R \}.$$

On a :

$$\begin{aligned} U \cdot V &= \rho A \cdot (\lambda B + \mu \cdot C) \\ &= \rho\lambda \cdot (A \cdot B) + \rho\mu \cdot (A \cdot C). \end{aligned}$$

Or :

$$(F \perp F') \Leftrightarrow (\forall \rho)(\forall \lambda)(\forall \mu) \quad U \cdot V = 0$$
$$\Leftrightarrow A \cdot B = 0 \quad \text{et} \quad A \cdot C = 0$$
$$\Leftrightarrow A \perp B \quad \text{et} \quad A \perp C$$

Et :

Pour qu'une variété F de dimension 1 soit orthogonale à une variété F′ de dimension 2, il faut et il suffit qu'un vecteur A de F soit orthogonal à deux vecteurs B et C linéairement indépendants de F′.

417. Orthogonalisation de Schmidt.

Un système de plusieurs vecteurs est dit orthonormé si les vecteurs qui le composent sont unitaires et deux à deux orthogonaux.

Les bases orthonormées sont donc des systèmes orthonormés.

L'orthogonalisation de Schmidt est une méthode permettant de construire des systèmes orthonormés, donc aussi des bases orthonormées.

1° **Soit un vecteur quelconque U non nul.**

Le vecteur

$$u = \frac{1}{\| U \|} \cdot U$$

est unitaire car

$$\| u \|^2 = u^2$$
$$= \frac{1}{\| U \|^2} \cdot U^2$$
$$= 1.$$

2° **Soit un vecteur unitaire $u \cdot (\| u \| = 1)$.**

Soit un vecteur V quelconque, mais linéairement indépendant de u. On considère le vecteur

$$N_1 = V - (V \cdot u) \cdot u$$

On a :

$$N_1 \cdot u = V \cdot u - (V \cdot u) \cdot u^2$$
$$= V \cdot u - V \cdot u$$
$$= 0.$$

Donc :

N_1 est orthogonal à u.

Le vecteur

$$v = \frac{N_1}{\| N_1 \|}$$

est unitaire, et par suite le système $\{u; v\}$ est orthonormé :

Et :

Etant donné un vecteur unitaire* u, *on peut trouver un vecteur unitaire* v *tel que le système* $\{\mathbf{u}; \mathbf{v}\}$ *soit orthonormé.

Si les vecteurs sont dans l'espace vectoriel R^2, on peut énoncer :

Etant donné dans R^2 un vecteur unitaire* u, *on peut trouver un vecteur unitaire* v *tel que* $\mathcal{B} = \{\mathbf{u}; \mathbf{v}\}$ *soit une base orthonormée.

3° Soient maintenant dans l'espace vectoriel R^3 un système orthonormé $\{u; v\}$.

Si W est un vecteur quelconque, linéairement indépendant de u et v, (Det $(u; v; W) \neq 0$) on considère le vecteur :

$$N_2 = W - (W \cdot u) \cdot u - (W \cdot v) \cdot v$$

On a :

$$\begin{aligned} N_2 \cdot u &= W \cdot u - (W \cdot u) \cdot u^2 - (W \cdot v) \cdot (v \cdot u) \\ &= W \cdot u - W \cdot u \\ &= 0. \end{aligned}$$

Donc N_2 est orthogonal au vecteur u.
On montre de même que N_2 est orthogonal au vecteur v.

Le vecteur

$$w = \frac{N_2}{\|N_2\|}$$

est unitaire, et par suite le système $\{u; v; w\}$ est orthonormé et par suite est une base de R^3.

Et :

Etant donné dans R^3 un système orthonormé* $\{\mathbf{u}; \mathbf{v}\}$, *on peut trouver un vecteur unitaire* w *tel que* $\mathcal{B} = \{\mathbf{u}; \mathbf{v}; \mathbf{w}\}$ *soit une base orthonormée.

En tenant compte du 2° :

Etant donné dans R^3 un vecteur unitaire* u *on peut trouver deux vecteurs unitaires* v *et* w *tels que* $\mathcal{B} = \{\mathbf{u}; \mathbf{v}; \mathbf{w}\}$ *soit une base orthonormée.

418. Ensemble des vecteurs orthogonaux à une variété.

Soit une variété F; on dit qu'un vecteur U est orthogonal à F si U est orthogonal à tous les vecteurs de F.

Etant donné une variété F, on se propose de déterminer l'ensemble des vecteurs orthogonaux à F.

1° *Dans R^2, on considère la variété linéaire F déterminée par le vecteur unitaire u :*

$$F = \{ U/U = \lambda \cdot u, \lambda \in R \}.$$

Soit v le vecteur orthogonal à u, tel que $\mathcal{B} = \{u; v\}$ est une base orthonormée. Un vecteur V quelconque de R^2 est donné par

$$V = X \cdot u + Y \cdot v$$

On a :

$$V \perp U \Leftrightarrow V \cdot u = 0$$
$$\Leftrightarrow (X \cdot u + Y \cdot v) \cdot u = 0$$
$$\Leftrightarrow X = 0.$$

Donc :

Pour qu'un vecteur V soit orthogonal à F, il faut et il suffit qu'il s'écrive $V = Y \cdot v$.

Et :

L'ensemble $F^\perp$ des vecteurs orthogonaux à F est la variété de dimension 1 déterminée par le vecteur v (ou par un vecteur quelconque orthogonal à F).

2° *Dans R^3, on considère la variété linéaire F déterminée par le vecteur unitaire u :*

$$F = \{ U/U = \lambda \cdot u, \lambda \in R \}.$$

Soit v, w deux vecteurs tels que $\mathcal{B} = \{u; v; w\}$ est une base orthonormée. Un vecteur V quelconque de R^3 est donné par

$$V = X \cdot u + Y \cdot v + Z \cdot w.$$

On a :

$$V \perp U \Leftrightarrow V \cdot u = 0$$
$$\Leftrightarrow (X \cdot u + Y \cdot v + Z \cdot w) \cdot u = 0$$
$$\Leftrightarrow X = 0.$$

Donc :

Pour qu'un vecteur V soit orthogonal à F, il faut et il suffit qu'il s'écrive $V = Y \cdot v + Z \cdot w$.

Et :

L'ensemble $F^\perp$ des vecteurs orthogonaux à F est la variété de dimension 2 déterminée par les vecteurs v et w (ou par deux vecteurs quelconques linéairement indépendants et orthogonaux à F).

3° *Dans R^3, on considère la variété F déterminée par le système orthonormé $\{u; v\}$:*

$$F = \{U/U = \lambda \cdot u + \mu \cdot v, \lambda \in R, \mu \in R\}$$

Soit v un vecteur tel que $\mathcal{B} = \{u; v; w\}$ soit une base orthonormée. Un vecteur V quelconque de R^3 est donné par

$$V = X \cdot u + Y \cdot v + Z \cdot w.$$

On a :

$$V \perp U \Leftrightarrow V \cdot u = 0 \quad \text{et} \quad V \cdot v = 0.$$

Or :

$$V \cdot u = (X \cdot u + Y \cdot v + Z \cdot w) \cdot u = X$$

et

$$V \cdot v = (X \cdot u + Y \cdot v + Z \cdot w) \cdot v = Y.$$

Donc :

$$(V \perp U) \Leftrightarrow (X = 0 \quad \text{et} \quad Y = 0)$$

Et :

Pour qu'un vecteur V soit orthogonal à F, il faut et il suffit qu'il s'écrive $V = Z \cdot w$.

Par suite :

L'ensemble $F^\perp$ des vecteurs orthogonaux à F est la variété de dimension 1 déterminée par le vecteur w (ou par un vecteur quelconque orthogonal à F).

419. Calcul du produit scalaire dans une base orthonormée.

Le produit scalaire a été défini dans la base canonique $\mathcal{B}_0 = \{i; j; k\}$; il peut être utile de calculer le produit scalaire de deux vecteurs donnés dans une base quelconque orthonormée $\mathcal{B} = \{u; v; w\}$.

Soient donc deux vecteurs V et V' tels que, dans $\mathcal{B}_0$,

$$\begin{cases} V = x \cdot i + y \cdot j + z \cdot k \\ V' = x' \cdot i + y' \cdot j + z' \cdot k \end{cases}$$

D'après la définition du n° 407, on a:

$$V \cdot V' = xx' + yy' + zz'. \qquad (419; 1)$$

D'autre part, dans la base orthonormée $\mathcal{B}$.

$$\begin{cases} V = X \cdot u + Y \cdot v + Z \cdot w \\ V' = X' \cdot u + Y' \cdot v + Z' \cdot w. \end{cases}$$

D'où :

$$V\ V' = (X \cdot u + Y \cdot v + Z w)\ (X' \cdot u + Y' \cdot v + Z' \cdot w)$$

En développant le produit, et en remarquant que

$$u^2 = 1, \quad v^2 = 1, \quad w^2 = 1, \quad uv = 0 \quad uw = 0 \quad v\,w = 0$$

on obtient :

$$V \cdot V' = XX' + Y\,Y' + ZZ' \qquad (419; 2)$$

Autrement dit :

Le produit scalaire de deux vecteurs s'évalue de la même façon dans les bases orthonormées,

ou :

Le produit scalaire est intrinsèque.

Par suite :

La norme d'un vecteur, l'orthogonalité des vecteurs sont intrinsèques.

420. Cosinus d'un bivecteur de R^2 ou de R^3.

Dans l'espace euclidien R^3 (ou dans R^2), on considère le bivecteur $(V; V')$ avec

$$\begin{cases} V = (x; y; z) \\ V' = (x'; y'; z') \end{cases}$$

On appelle cosinus du bivecteur $(V; V')$ le nombre réel

$$\cos (V; V') = \frac{V \cdot V'}{\| V\| \cdot \| V'\|} \qquad (420; 1)$$

On a donc :

$$\cos (V; V') = \frac{xx' + yy' + zz'}{\sqrt{x^2 + y^2 + z^2} \cdot \sqrt{x'^2 + y'^2 + z'^2}}. \qquad (420; 2)$$

De l'inégalité de Schwarz :

$$| V \cdot V' | \leqslant \| V\| \cdot \| V'\|$$

on tire :

$$\frac{| V \cdot V' |}{\| V\| \cdot \| V'\|} \leqslant 1.$$

D'où :

$$-1 \leqslant \frac{V \cdot V'}{\| V\| \cdot \| V'\|} \leqslant +1.$$

On a donc :

$$-1 \leqslant \cos (V; V') \leqslant +1. \qquad (420; 3)$$

421. Première identité de Lagrange.

En développant les produits et les carrés on vérifie facilement l'identité suivante, appelée première identité de Lagrange.

$$(x^2 + y^2)(x'^2 + y'^2) - (xx' + yy'')^2 = (xy' - yx')^2 \qquad (421; 1)$$

Vectoriellement elle s'écrit, dans l'espace R^2;

$$\| V\|^2 \cdot \| V'\|^2 - (V \cdot V')^2 = [\mathrm{Det}(V; V')]^2. \qquad (421; 2)$$

422. Sinus d'un bivecteur de R^2.

Dans l'espace euclidien R^2, on considère le bivecteur (V; V') avec

$$\begin{cases} V = (x\,; y) \\ V' = (x'\,; y') \end{cases}$$

On appelle *sinus* du bivecteur (V; V') le nombre réel

$$\sin(V; V') = \frac{\operatorname{Det}(V; V')}{\|V\| \cdot \|V'\|}. \qquad (422\,;1)$$

On a donc :

$$\sin(V\,; V') = \frac{xy' - yx'}{\sqrt{x^2 + y^2} \cdot \sqrt{x'^2 + y'^2}}. \qquad (422\,;2)$$

La formule (421 ; 2) montre que :

$$\|V\|^2 \cdot \|V'\|^2 \geqslant [\operatorname{Det}(V\,; V')]^2$$

ou

$$\|V\| \cdot \|V'\| \geqslant |\operatorname{Det}(V\,; V')|$$

ou

$$\frac{|\operatorname{Det}(V\,; V')|}{\|V\| \cdot \|V'\|} \leqslant 1.$$

On a donc :

$$-1 \leqslant \sin(V\,; V') \leqslant +1 \qquad (422\,;3)$$

423. Relation entre le cosinus et le sinus d'un bivecteur de R^2.

La formule (421 ; 2) s'écrit :

$$(V \cdot V')^2 + [\operatorname{Det}(V\,; V')]^2 = \|V\|^2 \cdot \|V'\|^2$$

ou

$$\frac{(V \cdot V')^2}{\|V\|^2 \cdot \|V'\|^2} + \frac{[\operatorname{Det}(V\,; V')]^2}{\|V\|^2 \cdot \|V'\|^2} = 1$$

ou encore :

$$\cos^2(V; V') + \sin^2(V; V') = 1. \qquad (423\,;1)$$

424. Produit vectoriel de deux vecteurs de R^3.

Dans l'espace euclidien, rapporté à la base canonique $\mathcal{B}_0$, on considère les deux vecteurs V et V' :

$$\begin{cases} V = (x\,; y\,; z) \\ V' = (x'\,; y'\,; z') \end{cases}$$

On appelle produit vectoriel des vecteurs V et V′, le vecteur W = (L; M; N) de R^3 dont les coordonnées dans la base canonique $\mathcal{B}_0$ sont :

$$L = \begin{vmatrix} y & y' \\ z & z' \end{vmatrix} \qquad M = \begin{vmatrix} z & z' \\ x & x' \end{vmatrix} \qquad N = \begin{vmatrix} x & x' \\ y & y' \end{vmatrix}$$

ou

$$L = yz' - zy' \qquad M = zx' - xz' \qquad N = xy' - yx'$$

On note :

$$W = V \wedge V'$$

et on lit « V vectoriel V′ ».

◇ *Exemple 1.*

Soient les vecteurs $u = \left(\frac{2}{3}; \frac{2}{3}; \frac{1}{3}\right)$ et $v = \left(-\frac{2}{3}; \frac{1}{3}; \frac{2}{3}\right)$. *Calculer* $u \wedge v$.

On a :

$$L = \begin{vmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{vmatrix} = \frac{3}{9} = \frac{1}{3}$$

$$M = \begin{vmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & -\frac{2}{3} \end{vmatrix} = -\frac{6}{9} = -\frac{2}{3}$$

$$N = \begin{vmatrix} \frac{2}{3} & -\frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} \end{vmatrix} = \frac{6}{9} = \frac{2}{3}.$$

Donc le vecteur $w = u \wedge v$ est :

$$w = \left(\frac{1}{3}; -\frac{2}{3}; \frac{2}{3}\right).$$

◇ *Exemple 2.*

Soient i, j, k *les vecteurs de la base canonique; calculer* $i \wedge j$; $j \wedge k$ et $k \wedge i$.

On a :

$$i = (1; 0; 0) \qquad j = (0; 1; 0)$$

Les coordonnées de $i \wedge j$ sont donc :

$$l = \begin{vmatrix} 0 & 1 \\ 0 & 0 \end{vmatrix} = 0$$

$$m = \begin{vmatrix} 0 & 0 \\ 1 & 0 \end{vmatrix} = 0$$

$$n = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1$$

Donc :

$$\mathbf{i} \wedge \mathbf{j} = \mathbf{k} \qquad (424;\ 1)$$

De même :

$$\mathbf{j} \wedge \mathbf{k} = \mathbf{i} \qquad (424;\ 2)$$
$$\mathbf{k} \wedge \mathbf{i} = \mathbf{j}. \qquad (424;\ 3)$$

425. Propriétés du produit vectoriel.

Le produit vectoriel possède les propriétés suivantes :

1° On a :

$$W = V \wedge V'$$

et les coordonnées de W sont :

$$L = \begin{vmatrix} y & y' \\ z & z' \end{vmatrix} \qquad M = \begin{vmatrix} z & z' \\ x & x' \end{vmatrix} \qquad N = \begin{vmatrix} x & x' \\ y & y' \end{vmatrix}$$

D'autre part, les coordonnées de $V' \wedge V$ sont :

$$L' = \begin{vmatrix} y' & y \\ z' & z \end{vmatrix} \qquad M = \begin{vmatrix} z' & z \\ x' & x \end{vmatrix} \qquad N = \begin{vmatrix} x' & x \\ y' & y \end{vmatrix}$$

c'est-à-dire :

$$L' = -L \qquad M' = -M \qquad N' = -N$$

Par suite :

$$\boldsymbol{V' \wedge V = -(V \wedge V')}. \qquad (425;\ 1)$$

Et :

Le produit vectoriel est anticommutatif ou alterné.

2° On a :

$$\begin{aligned} V \cdot W &= x\,(yz' - zy') + y\,(zx' - xz') + z\,(xy' - yx') \\ &= xyz' - xzy' + yzx' - xyz' + xzy' - yzx' \\ &= 0. \end{aligned}$$

Donc :

$$\boldsymbol{W \perp V}.$$

On démontre de même :

$$\boldsymbol{W \perp V'}.$$

Et :

Le produit vectoriel de deux vecteurs est orthogonal à ces deux vecteurs.

3° On a :

$$\text{Det}(V;V';W) = \begin{vmatrix} x & x' & L \\ y & y' & M \\ z & z' & N \end{vmatrix}$$

$$= xy'N + yz'L + zx'M - zy'L - yx'N - xz'N$$
$$= (yz' - yz')\,L + (zx' - xy')\,M + (xy' - yx')\,N$$
$$= L^2 + M^2 + N^2.$$

Donc :

$$\text{Det}(V;V';W) = L^2 + M^2 + N^2 \qquad (425;2)$$

ou

$$\text{Det}(V;V';W) = \|W\|^2 \qquad (425;3)$$

Ainsi, comme le déterminant Det(V; V';W) est positif :

Le trivecteur (V; V'; W) est orienté positivement.

4° Si $V' = \lambda V$ on a :

$$L = \begin{vmatrix} y & \lambda y \\ z & \lambda z \end{vmatrix} = 0$$

$$M = \begin{vmatrix} z & \lambda z \\ x & \lambda x \end{vmatrix} = 0$$

$$N = \begin{vmatrix} x & \lambda x \\ y & \lambda y \end{vmatrix} = 0.$$

Donc :

$$\boldsymbol{V'} = \lambda\cdot\boldsymbol{V} \Rightarrow \boldsymbol{V}\wedge\boldsymbol{V'} = 0. \qquad (425;4)$$

5° Soient les vecteurs λV et $\mu V'$. Le produit vectoriel $(\lambda V)\wedge(\mu V')$ a pour coordonnées

$$L' = \begin{vmatrix} \lambda y & \mu y' \\ \lambda z & \mu z' \end{vmatrix} = \lambda\mu\cdot\begin{vmatrix} y & y' \\ z & z' \end{vmatrix} = \lambda\mu\cdot L$$

$$M' = \begin{vmatrix} \lambda z & \mu z' \\ \lambda x & \mu x' \end{vmatrix} = \lambda\mu\cdot\begin{vmatrix} z & z' \\ x & x' \end{vmatrix} = \lambda\mu\cdot M$$

$$N' = \begin{vmatrix} \lambda x & \mu x' \\ \lambda y & \mu y' \end{vmatrix} = \lambda\mu\cdot\begin{vmatrix} x & x' \\ y & y' \end{vmatrix} = \lambda\mu\cdot N.$$

D'où la formule :

$$(\lambda\boldsymbol{V})\wedge(\mu\boldsymbol{V'}) = \lambda\mu\cdot(\boldsymbol{V}\wedge\boldsymbol{V'}) \qquad (425;5)$$

6° Soient les vecteurs :

$$V = (x;y;z) \qquad V' = (x';y';z') \qquad V'' = (x'';y'';z'').$$

Les coordonnées du vecteur $V \wedge (V' + V'')$ sont :

$$L_1 = \begin{vmatrix} y & y' + y'' \\ z & z' + z'' \end{vmatrix} = \begin{vmatrix} y & y' \\ z & z' \end{vmatrix} + \begin{vmatrix} y & y'' \\ z & z'' \end{vmatrix}$$

$$M_1 = \begin{vmatrix} z & z' + z'' \\ x & x' + x'' \end{vmatrix} = \begin{vmatrix} z & z' \\ x & x' \end{vmatrix} + \begin{vmatrix} z & z'' \\ x & x'' \end{vmatrix}$$

$$M_2 = \begin{vmatrix} x & x' + x'' \\ y & y' + y'' \end{vmatrix} = \begin{vmatrix} x & x' \\ y & y' \end{vmatrix} + \begin{vmatrix} x & x'' \\ y & y'' \end{vmatrix}$$

D'autre part, les coordonnées du vecteur $V \wedge V' + V \wedge V''$ sont :

$$L_2 = \begin{vmatrix} y & y' \\ z & z' \end{vmatrix} + \begin{vmatrix} y & y'' \\ z & z'' \end{vmatrix}$$

$$M_2 = \begin{vmatrix} z & z' \\ x & x' \end{vmatrix} + \begin{vmatrix} z & z'' \\ x & x'' \end{vmatrix}$$

$$N_2 = \begin{vmatrix} x & x' \\ y & y' \end{vmatrix} + \begin{vmatrix} x & x'' \\ y & y'' \end{vmatrix}$$

Donc :

$$L_1 = L_2 \qquad M_1 = M_2 \qquad N_1 = N_2$$

ou :

$$V \wedge (V' + V'') = V \wedge V' + V \wedge V''. \qquad (425;5)$$

De même :

$$(V + V') \wedge V'' = V \wedge V'' + V' \wedge V'' \qquad (425;6)$$

Et :

Le produit vectoriel est distributif pour l'addition des vecteurs :

7° Des résultats précédents on déduit :

$$(U + V) \wedge (U + V) = 0$$
$$(U - V) \wedge (U - V) = 0$$

Et :

$$(U - V) \wedge (U + V) = U \wedge U + U \wedge V - V \wedge U - V \wedge V$$

ou

$$(U - V) \wedge (U + V) = 2 \cdot (U \wedge V) \qquad (425;7)$$

et

$$(U + V) \wedge (U - V) = -2 \cdot (U \wedge V) \qquad (425;8)$$

426. Seconde identité de Lagrange.

En développant les produits et les carrés on vérifie facilement l'identité suivante, appelée seconde identité de Lagrange :

$$(x^2 + y^2 + z^2)(x'^2 + y'^2 + z'^2) - (xx' + yy' + zz')^2$$
$$= (yz' - zy')^2 + (zx' - xz')^2 + (xy' - yx')^2 \qquad (426;1)$$

Vectoriellement elle s'écrit, dans l'espace R^3 :

$$\| V \|^2 \cdot \| V' \|^2 - (V \cdot V')^2 = \| V \wedge V' \|^2 \qquad (426;2)$$

427. Base orthonormée positive et produit vectoriel.

1° Soit un système orthonormé $\{u; v\}$:

$$\|u\| = 1 \qquad \|v\| = 1 \qquad u \perp v.$$

On considère le vecteur $u \wedge v$; on a :

$$u \perp (u \wedge v) \qquad v \perp (u \wedge v),$$

et

$$\|u \wedge v\|^2 = \|u\|^2 \cdot \|v\|^2 - (u \cdot v)^2 = 1$$

ou

$$\|u \wedge v\| = 1.$$

De plus :

$$\mathrm{Det}\,(u\,;v\,;u \wedge v) = \|u \wedge v\|^2 = 1.$$

Donc :

Si $\{u; v\}$ est un système orthonormé, le système $\{u; v; u \wedge v\}$ est une base orthonormée positive.

2° On considère une base orthonormée positive $\{u; v; w\}$. Puisque $\{u; v; u \wedge v\}$ est une base orthonormée positive, on en déduit :

et aussi

$$\left.\begin{array}{l} w = u \wedge v \\ u = v \wedge w \\ v = w \wedge u \end{array}\right\} \qquad (427\,;1)$$

3° Par suite *si $\mathcal{B} = \{u; v; w\}$ est une base orthonormée positive, on a*

$$\mathrm{Det}\,(u\,;v\,;w) = 1. \qquad (427\,;2)$$

428. Calcul du produit vectoriel dans une base orthonormée positive.

Le produit vectoriel a été défini dans la base canonique $\mathcal{B}_0 = \{i; j; k\}$; il peut être utile de calculer le produit vectoriel de deux vecteurs donnés dans une base quelconque orthonormée positive $\mathcal{B} = \{u; v; w\}$.

Soient donc deux vecteurs V et V′ tels que

$$\begin{array}{l} V = x \cdot i + y \cdot j + z \cdot k \\ V' = x' \cdot i + y' \cdot j + z' \cdot k \end{array}$$

On a dans $\mathcal{B}_0$:

$$V \wedge V' = (yz' - zy') \cdot i + (zx' - xz') \cdot j + (xy' - yx') \cdot k$$

D'autre part dans la base orthonormée positive $\mathcal{B}$:

$$\begin{array}{l} V = X \cdot u + Y \cdot v + Z \cdot w \\ V' = X' \cdot u + Y' \cdot v + Z' \cdot w \end{array}$$

D'où :

$$\begin{aligned} V\wedge V' &= (Xu + Yv + Zw) \wedge (X'u + Y'v + Z'w) \\ &= (YZ' - ZY') \cdot (v\wedge w) + (ZX' - XZ') \cdot (w\wedge u) \\ &\quad + (XY' - YX') \cdot (u\wedge v). \end{aligned}$$

Or : $v\wedge w = u, \quad w\wedge u = v \quad$ et $\quad u\wedge v = w.$

Donc : $V\wedge V' = (YZ' - ZY') \cdot u + (ZX' - XZ')\, v + (XY' - YX') \cdot w.$

Autrement dit :

Le produit vectoriel de deux vecteurs s'évalue de la même façon dans des bases orthonormées positives,

ou :

Le produit vectoriel est intrinsèque.

429. Sinus d'un bivecteur de R^3.

Dans l'espace euclidien R^3, on considère le bivecteur (V; V′) avec

$$\begin{cases} V = (x ; y ; z) \\ V' = (x' ; y' ; z') \end{cases}$$

On appelle sinus du bivecteur (V; V′) le nombre réel

$$\mathbf{sin}\,(V; V') = \frac{\| V\wedge V' \|}{\| V \| \cdot \| V' \|} \qquad (429; 1)$$

c'est-à-dire :

$$\sin\,(V; V') = \frac{\sqrt{L^2 + M^2 + N^2}}{\sqrt{x^2 + y^2 + z^2} \cdot \sqrt{x'^2 + y'^2 + z'^2}}. \qquad (429; 2)$$

Donc :

Dans l'espace R^3, le sinus d'un bivecteur est positif.

La formule (426; 2) montre que

$$\| V\wedge V' \|^2 \leqslant \| V \|^2 \cdot \| V' \|^2$$

ou

$$\| V\wedge V' \| \leqslant \| V \| \cdot \| V' \|.$$

Par suite :

$$0 \leqslant \sin\,(V; V') \leqslant 1 \qquad (429; 3)$$

430. Relation entre le cosinus et le sinus d'un bivecteur de R^3.

De la formule (426; 2) on déduit :

$$(V \cdot V')^2 + \| V\wedge V' \|^2 = \| V \|^2 \cdot \| V' \|^2$$

ou

$$\frac{(V \cdot V')^2}{\|V\|^2 \cdot \|V'\|^2} + \frac{\|V \wedge V'\|^2}{\|V\|^2 \cdot \|V'\|^2} = 1$$

ou encore

$$\cos^2(V; V') + \sin^2(V; V') = 1. \qquad (430; 1)$$

431. Nouvelle expression de la norme d'un produit vectoriel.

La formule (426; 2) :

$$\|V \wedge V'\|^2 = \|V\|^2 \cdot \|V'\|^2 - (V \cdot V')^2$$

s'écrit :

$$\|V \wedge V'\|^2 = \|V\|^2 \cdot \|V'\|^2 \cdot \left(1 - \frac{(V \cdot V')^2}{\|V\|^2 \cdot \|V'\|^2}\right)$$
$$= \|V\|^2 \cdot \|V'\|^2 \cdot [1 - \cos^2(V; V')]$$
$$= \|V\|^2 \cdot \|V'\|^2 \cdot \sin^2(V; V').$$

D'où :

$$\|V \wedge V'\| = \|V\| \cdot \|V'\| \cdot \sin(V; V') \qquad (431; 1)$$

432. Produit mixte.

1° Soient trois vecteurs A, B, C de R^3. On considère le produit vectoriel $A \wedge B$.

On appelle produit mixte des trois vecteurs A, B, C le produit scalaire du vecteur A ∧ B et du vecteur C.

C'est donc le nombre réel $p = (A \wedge B) \cdot C$.

2° On a ;

$$(A \wedge B) . C = (yz' - zy') \cdot x'' + (zx' - xz') \cdot y'' + (xy' - yx') \cdot z''$$
$$= yz'x'' - zy'x'' + zx'y'' - xz'y'' + xy'z'' - yx'z''$$
$$= \text{Det}(A; B; C).$$

Donc :

$$(A \wedge B) \cdot C = \text{Det}(A; B; C) \qquad (432; 1)$$

De même :

$$A \cdot (B \wedge C) = \text{Det}(A; B; C). \qquad (432; 2)$$

3° *Le produit mixte est intrinsèque*, c'est-à-dire qu'il ne dépend pas de la base orthonormée positive utilisée pour la calculer, puisque dans ces conditions les produits scalaire et vectoriel sont intrinsèques.

4° En conséquence :

Le déterminant de trois vecteurs ne dépend pas de la base orthonormée positive utilisée pour le calculer.

CHAPITRE XXXIII

POLYNOMES FORMELS A UNE INDÉTERMINÉE

433. Polynômes sur un anneau ou sur un corps.

Dans ce qui suit K désigne un anneau commutatif unitaire ou un corps commutatif.

On appelle polynôme formel sur K une suite infinie d'éléments de K telle qu'à partir d'un certain rang tous les éléments de la suite sont nuls.

◇ *Exemples.*

1° $A = (1; 3; 0; -5; 0; 0; ...)$

est un polynôme formel sur l'anneau Z.

2° $A = (0; \sqrt{3}; 0; -\sqrt{5}; 7; 0; 0; ...)$

est un polynôme formel sur le corps R.

3° $A = (i; 3; 1 - i; 0; 0; 1 + i; 0; 0; ...)$

est un polynôme formel sur le corps C.

4° $A = (\dot{0}; \dot{2}; \dot{3}; \dot{1}; \dot{0}; \dot{0}; ...)$

est un polynôme formel sur le corps $K = Z/5$.

Un polynôme sera noté :

$$A = (a_0; a_1; a_2; ...; a_n; 0; 0; ...)$$

Tous les nombres suivants a_n *sont nuls. Les nombres* $a_0; a_1; ...; a_n$ *sont les coefficients du polynôme.*

434. Polynômes identiques ou égaux.

Deux polynômes A et B sont égaux ou identiques s'ils ont les mêmes coefficients.

Si :

$A = (a_0; a_1; a_2; ...; a_n; 0; 0; ...)$ et $B = (b_0; b_1; b_2; ...; b_n; 0; 0 ...)$

on a l'équivalence

$$(A = B) \Leftrightarrow [(\forall i) : a_i = b_i)].$$

435. Addition des polynômes.

Soient les polynômes :

$$A = (a_0; a_1; ...; b_n; 0; 0; ...)$$

et

$$B = (b_0; b_1; ...; b_n; 0; 0; ...).$$

On appelle somme des polynômes A et B le polynôme S :

$$S = A + B = (a_0 + b_0; a_1 + b_1; ... a_n + b_n; ...)$$

◇ *Exemple.*

Soient :

$$A = (1 + i; 2; 1 - i; 0; 0; ...)$$
$$B = (-2; i; 4 - 2i; 3; 0; 0; ...)$$

Calculer A + B.

On a :

$$A + B = (-1 + i; 2 + i; 5 - 3i; 3; 0; 0; ...).$$

436. Propriétés de l'addition des polynômes.

L'addition possède les propriétés suivantes :

Commutativité.

On a :

$$A + B = (a_0 + b_0; a_1 + b_1; ...; a_i + b_i; ...)$$

et

$$B + A = (b_0 + a_0; b_1 + a_1; ...; b_i + a_i; ...)$$

Comme $a_i + b_i = b_i + a_i$ les deux résultats sont identiques. Donc :

[C] $$(\forall A)(\forall B) \quad A + B = B + A \qquad (436; 1)$$

Et :

L'addition des polynômes est commutative.

Associativité.

On a :

$$(A + B) + C = (a_0 + b_0; a_1 + b_1 + ...) + (c_0; c_1; ...)$$
$$= (a_0 + b_0 + c_0; a_1 + b_1 + c_1; ...)$$

et $$\begin{aligned} A + (B + C) &= (a_0; a_1; ...) + (b_0 + c_0; b_1 + c_1; ...) \\ &= (a_0 + b_0 + c_0; a_1 + b_1 + c_1; ...) \end{aligned}$$

Les résultats sont identiques. Donc :

[A] $(\forall A)(\forall B)(\forall C)\quad (A + B) + C = A + (B + C)$ (436; 2)

L'addition des polynômes est associative.

Existence d'un polynôme neutre pour l'addition.

Soit le polynome :

$$A = (a_0; a_1; ...; a_n; 0; 0; ...)$$

On envisage le polynôme :

$$E = (0; 0; 0; ...)$$

On a :

$$\begin{aligned} A + E &= (a_0 + 0; a_1 + 0; ...; a_n + 0; 0; 0; ...) \\ &= (a_0; a_1; ...; a_n; ...) \\ &= A. \end{aligned}$$

En tenant compte de la commutativité, on a :

[N] $(\exists E)(\forall A)\quad A + E = E + A = A.$ (436; 3)

La loi étant additive, on note E = 0. Donc :

$$(\forall A)\quad A + 0 = 0 + A = A. \qquad (436; 4)$$

L'ensemble des polynômes est symétrisé pour l'addition.

Soit le polynôme :

$$A = (a_0; a_1; ...; a_n; 0; 0; ...)$$

On considère le polynôme :

$$A' = (-a_0; -a_1; ...; -a_n; 0; 0; ...)$$

On a :

$$\begin{aligned} A + A' &= (a_0 + (-a_0); a_1 + (-a_1); ...; a_n + (-a_n); 0; 0; ...) \\ &= (0; 0; ...; 0; 0; 0; ...) \\ &= 0. \end{aligned}$$

En tenant compte de la commutativité, on a :

[S] $(\forall A)(\exists A')\quad A + A' = A' + A = 0.$ (436; 5)

Et :

Tous les polynômes ont un polynôme symétrique pour l'addition.

On note : $A' = -A$; et *— A est le polynôme opposé du polynôme A.*

437. Groupe additif des polynômes.

Soit l'ensemble des polynômes construits sur l'anneau K ou le corps K. On le note $\mathcal{P}$ (K) ou simplement $\mathcal{P}$.

Cet ensemble est muni d'une addition possédant les propriétés [A] [N] [S] [C]. Donc :

L'ensemble $\mathcal{P}$ des polynômes est un groupe additif commutatif.

438. Régularité.

Soient trois polynômes A, B et M.

On suppose que l'on a :

$$A + M = B + M.$$

En ajoutant $- M$ aux deux membres de cette égalité, on obtient :

$$(A + M) + (- M) = (B + M) + (- M)$$

ou

$$A + [M + (- M)] = B + [M + (- M)]$$

ou

$$A + 0 = B + 0$$

ou

$$A = B.$$

Donc :

$$(\forall A)(\forall B)(\forall M) \qquad A + M = B + M \Rightarrow A = B. \qquad (438;1)$$

Et :

Tous les polynômes sont réguliers pour l'addition.

439. Soustraction.

Soient deux polynômes A et B.

Trouver le polynôme X tel que $A = B + X$ s'appelle soustraire B de A.

En ajoutant $- B$ aux deux membres de l'égalité précédente, on obtient :

$$\begin{aligned}(- B) + A &= (- B) + (B + X)\\ &= [(- B) + B] + X\\ &= 0 + X\\ &= X.\end{aligned}$$

Le polynôme cherché est donc :

$$X = (-B) + A$$

ou

$$X = A + (- B).$$

Et :

Pour soustraire un polynôme on ajoute le polynôme opposé.

Le polynôme X est le polynôme-différence entre A et B. On le note :

$$X = A - B$$

D'où :

$$A - B = A + (-B).$$

440. Multiplication d'un polynôme par un scalaire.

Soient un scalaire λ ($\lambda \in K$) et un polynôme

$$A = (a_0; a_1; ...; a_n; 0; 0; ...)$$

On appelle produit du polynôme A par le nombre λ, le polynôme P;

$$P = (\lambda a_0; \lambda a_1; ...; \lambda a_n; 0; 0; ...)$$

On note :

$$P = \lambda \cdot A.$$

On définit ainsi une loi externe

$$f: \quad (\lambda; A) \in K \times \mathcal{P} \longrightarrow f(\lambda; A) = \lambda \cdot A \in \mathcal{P}.$$

◇ *Exemple 1.*

Soit $A = (1 + i; 2; -4; i; 0; 0; ...)$. *Calculer* $(1 - i) A$.

On a :

$$(1 - i) \cdot A = [(1 + i)(1 - i); 2(1 - i); -4(1 - i); i(1 - i); 0; 0; ...]$$
$$= (2; 2 - 2i; -4 + 4i; 1 + i; 0; 0; ...)$$

◇ *Exemple 2.*

Dans $\mathcal{P}(K)$ *avec* $K = Z/6$, *on donne le polynôme.*

$$A = (\dot{2}; -\dot{3}; \dot{4}; \dot{0}; \dot{0} ...).$$

Soit $\lambda = \dot{3}$. *Calculer* $\lambda \cdot A$.

On a :

$$\lambda \cdot A = (\dot{2} \cdot \dot{3}; -\dot{3} \cdot \dot{3}; \dot{4} \cdot \dot{3}; \dot{0}; \dot{0} ...)$$
$$= (\dot{0}; \dot{3}; \dot{0}; \dot{0}; \dot{0} ...)$$

441. Propriété de la multiplication d'un polynôme par un nombre.

On a immédiatement :

$$1 \cdot A = (1.a_0; 1.a_1; ...; 1.a_n; 0; 0; ...)$$
$$= (a_0; a_1; ...; a_n; 0; 0; ...)$$
$$= A.$$

Donc :

N' $\qquad (\forall A) \quad 1 \cdot A = A. \qquad$ (441 ; 1)

442. Multiplication des polynômes.

Soient les polynômes

$$A = (a_0; a_1; ...; a_i; ...; a_n; 0; 0; ...)$$

et

$$B = (b_0; b_1; ...; b_j; ...; b_m; 0; 0; ...)$$

On appelle produit du polynôme A par le polynôme B le polynôme Π ***:***

$$\Pi = AB = (\mathbf{p}_0; \mathbf{p}_1; ...; \mathbf{p}_k; ...; \mathbf{p}_{n+m}; 0; 0; ...)$$

avec

$$\mathbf{p}_0 = \mathbf{a}_0\mathbf{b}_0$$
$$\mathbf{p}_1 = \mathbf{a}_0\mathbf{b}_1 + \mathbf{a}_1\mathbf{b}_0$$
$$\mathbf{p}_2 = \mathbf{a}_0\mathbf{b}_2 + \mathbf{a}_1\mathbf{b}_1 + \mathbf{a}_2\mathbf{b}_0$$

. . . .

$$\mathbf{p}_k = \mathbf{a}_0\mathbf{b}_k + \mathbf{a}_1\mathbf{b}_{k-1} + ... + \mathbf{a}_{k-1}\mathbf{b}_1 + \mathbf{a}_k\mathbf{b}_0 = \sum_{i+j=k} \mathbf{a}_i\mathbf{b}_j$$

. . . .

Le tableau suivant donne le moyen de calculer pratiquement les coefficients p_k du produit $\Pi = AB$. En effet les coefficients p_k ne sont autres que les sommes des éléments des diagonales du tableau.

	b_0	b_1	b_2	------------	b_m	0	0
a_0	a_0b_0	a_0b_1	a_0b_2	------------	a_0b_m	0	0
a_1	a_1b_0	a_1b_1	a_1b_2	------------	a_1b_m	0	0
a_2	a_2b_0	a_2b_1	a_2b_2	------------	a_2b_m	0	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
a_n	a_nb_0	a_nb_1	a_nb_2	------------	a_nb_m	0	0
0	0	0	0	------------	0	0	0
0	0	0	0	------------	0	0	0

En dehors du rectangle mis en évidence il n'y a que des zéros. Le dernier coefficient qui peut n'être pas nul dans Π est $a_n b_m$.

◇ *Exemple 1.*

Soient dans $\mathcal{T}(Z)$ *les deux polynômes*

$$A = (2;\ -1;\ 3;\ 0;\ 0;\ \dots)$$

et

$$B = (-1;\ 4;\ 0;\ 0;\ \dots).$$

Calculer le produit AB.

Pour faciliter les calculs on construit le tableau suivant :

	-1	4	0	0
2	-2	8	0	0
-1	1	-4	0	0
3	-3	12	0	0
0	0	0	0	0
0	0	0	0	0

D'où, en sommant les diagonales montantes :

$$AB = (-2;\ 9;\ -7;\ 12;\ 0;\ 0;\ \dots)$$

◇ *Exemple 2.*

Soient dans $\mathcal{T}(C)$ *les deux polynômes*

$$A = (1 + i;\ 2;\ 0;\ 0;\ \dots)$$
$$B = (-2;\ 1 - i;\ -2i\ \ 0;\ 0;\ \dots).$$

Calculer le polynôme AB.

On utilise le tableau suivant :

	-2	1-i	-2i	0	0
1+i	-2-2i	2	2-2i	0	0
2	-4	2-2i	-4i	0	0
0	0	0	0	0	0
0	0	0	0	0	0

En sommant les diagonales on obtient :

$$AB = (-2 - 2i; -2; 4 - 4i; -4i; 0; 0; \ldots)$$

◇ *Exemple 3.*

On considère l'ensemble $\mathfrak{T}(K)$ avec $K = Z/6$. On donne

$$A = (\dot{2}; \dot{3}; \dot{2}; \dot{0}; \dot{0} \ldots)$$

et

$$B = (\dot{5}; \dot{3}; \dot{0}; \dot{0} \ldots)$$

Calculer le polynôme AB.

On construit le tableau suivant :

	$\dot{5}$	$\dot{3}$	$\dot{0}$	$\dot{0}$
$\dot{2}$	$\dot{4}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{3}$	$\dot{3}$	$\dot{3}$	$\dot{0}$	$\dot{0}$
$\dot{2}$	$\dot{4}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$

D'où :

$$AB = (\dot{4} ; \dot{3} ; \dot{1} ; \dot{0} ; \dot{0} ; ...)$$

443. Propriétés de la multiplication.

La multiplication des polynômes possède les propriétés suivantes :

Commutativité.

Soient les polynômes :

$$A = (a_0 ; a_1 ; ... ; a_n ; 0 ; 0 ; ...)$$

et

$$B = (b_0 ; b_1 ; ... ; b_m ; 0 ; 0 ; ...)$$

On a :

$$AB = (p_0 ; p_1 ; ... ; p_k ; ... ; p_{n+m} ; 0 ; 0 ...)$$

avec

$$p_k = \sum_{i+j=k} a_i b_j$$

et

$$BA = (q_0 ; q_1 ; ... ; q_k ; ... ; q_{n+m}\ 0 ; 0 ; ...)$$

avec

$$q_k = \sum_{i+j=k} b_j a_i$$

Comme :

$$(\forall k) \quad \sum_{i+j=k} a_i b_j = \sum_{i+j=k} b_j a_i$$

les deux résultats sont identiques. Donc :

[C] $$(\forall A)(\forall B) \quad AB = BA. \qquad (443 ; 1)$$

Et :

La multiplication des polynômes est commutative.

Associativité.

Soient les polynômes :

$$A = (a_0 ; a_1 ; ... ; a_i ; ...)$$
$$B = (b_0 ; b_1 ; ... ; b_j ; ...)$$
$$C = (c_0 ; c_1 ; ... ; c_k ; ...)$$

On a :

$$AB = (p_0 ; p_1 ; \cdots p_n ; \cdots)$$

avec
$$p_n = \sum_{i+j=n} a_i b_j$$

et
$$BC = (q_0 ; q_1 ; \ldots ; q_m ; \ldots)$$

avec
$$q_m = \sum_{j+k=m} b_j c_k.$$

Par suite, on en déduit :

$$(AB) \cdot C = (r_0 ; r_1 ; \ldots r_\lambda ; \ldots)$$

avec
$$r_\lambda = \sum_{n+k=\lambda} p_n c_k$$

$$= \sum_{n+k=\lambda} \left[c_k \left(\sum_{i+j=n} a_i b_j \right) \right]$$

$$= \sum_{i+j+k=\lambda} (a_i b_j c_k) \qquad (443 ; 1)$$

De même :

$$A \cdot (BC) = (s_0 ; s_1 ; \ldots ; s_\lambda ; \ldots)$$

avec
$$s_\lambda = \sum_{i+m=\lambda} a_i q_m$$

$$= \sum_{i+m=\lambda} \left[a_i \left(\sum_{j+k=m} b_j c_k \right) \right]$$

$$= \sum_{i+j+k=\lambda} (a_i b_j c_k) \qquad (443 ; 2)$$

Les résultats (443; 1) et 443; 2) sont identiques : $r_\lambda = s_\lambda$. Donc :

[A] $$(\forall A)(\forall B)(\forall C) \quad (AB) \cdot C = A \cdot (BC) \qquad (443 ; 3)$$

Et :

La multiplication des polynômes est associative.

Existence d'un polynôme neutre pour la multiplication.

Soit le polynôme :

$$A = (a_0 ; a_1 ; \ldots ; a_n ; 0 ; 0 ; \ldots)$$

On envisage le polynôme :

$$I = (1;0;0;\dots)$$

Pour calculer le produit AI on utilise le tableau suivant :

	1	0	0
a_0	a_0	0	0
a_1	a_1	0	0
⋮	⋮	⋮	⋮
a_n	a_n	0	0
0	0	0	0
0	0	0	0

On a donc :

$$AI = (a_0\,;a_1\,;\dots;a_n\,;0\,;0\,;\dots)$$
$$= A.$$

En tenant compte de la commutativité, on a :

N $$(\exists I)(\forall A) \qquad A\cdot I = I\cdot A = A.$$

La loi étant multiplicative on note I = 1, et I est le polynôme-unité.

Remarque.

Soit le polynôme :

$$A = (a\,;0\,;0\,;\dots)$$

On a :

$$A = a\cdot(1\,;0\,;0\,;\dots)$$
$$= 1 \times a.$$

On est donc amené à poser :

$$A = a.$$

A est dit polynôme constant.

444. Relations entre les diverses lois.

Distributivité de la multiplication pour l'addition.

Soient les polynômes :

$$A = (a_0 ; a_1 ; \dots ; a_j ; \dots)$$
$$B = (b_0 ; b_1 ; \dots ; b_j ; \dots)$$
$$M = (m_0 ; m_1 ; \dots m_i ; \dots).$$

On a : $$M(A + B) = (p_0 ; \dots ; p_k ; \dots)$$

avec $$p_k = \sum_{i+j=k} m_i(a_j + b_j)$$

et $$MA + MB = (q_0 ; \dots ; q_k ; \dots)$$

avec $$q_k = \sum_{i+j=k} m_i a_j + \sum_{i+j=k} m_i b_j = \sum_{i+j=k} m_i(a_j + b_j).$$

Les deux résultats sont identiques : $p_k = q_k$. Donc :

[D] $(\forall A)(\forall B)(\forall M) \qquad M \cdot (A + B) = MA + MB.$

Et :

La multiplication des polynômes est distributive pour l'addition des polynômes.

Distributivité de la loi externe pour l'addition dans $\mathcal{P}$(K).

Soient les polynômes A, B, et le nombre α ($\alpha \in$ K).

On a : $$\alpha(A + B) = (p_0 ; p_1 ; \dots ; p_k ; \dots)$$

avec $$p_k = \alpha(a_k + b_k)$$

et $$\alpha A + \alpha B = (q_0 ; q_1 ; \dots ; q_k ; \dots)$$

avec $$q_k = \alpha a_k + \alpha b_k = \alpha(a_k + b_k).$$

Les deux résultats sont identiques : $p_k = q_k$. Donc :

[D'] $(\forall \alpha)(\forall A)(\forall B) : \quad \alpha \cdot (A + B) = \alpha \cdot A + \alpha \cdot B.$

Et :

La multiplication d'un polynôme par un scalaire est distributive pour l'addition des polynômes.

Distributivité de la loi externe pour l'addition dans K.

Soient le polynôme A et les nombres α et β. ($\alpha \in K$; $\beta \in K$).

On a :

$$(\alpha + \beta) \cdot A = (p_0 ; p_1 ; \dots ; p_k ; \dots)$$

avec
$$p_k = (\alpha + \beta)\, a_k$$

et
$$\alpha \cdot A + \beta \cdot A = (q_0 ; q_1 ; \dots ; q_k ; \dots)$$

avec
$$q_k = \alpha \cdot a_k + \beta \cdot a_k.$$
$$= (\alpha + \beta) \cdot a_k.$$

Les deux résultats sont identiques : $p_k = q_k$. Donc :

[D''] $\quad (\forall \alpha)(\forall \beta)(\forall A) \qquad (\alpha + \beta) \cdot A = \alpha \cdot A + \beta \cdot A.$

Et :

La multiplication d'un polynôme par un scalaire est distributive pour l'addition des scalaires.

Associativité mixte de la loi externe et de la multiplication des scalaires.

Soient les scalaires α, β et le polynôme A.

On a :

$$\alpha(\beta \cdot A) = (p_0 ; p_1 ; \dots ; p_k ; \dots)$$

avec
$$p_k = \alpha(\beta \cdot a_k)$$
$$= \alpha \cdot \beta a_k$$

et
$$(\alpha\beta) \cdot A = (q_0 ; q_1 ; \dots ; q_k ; \dots.)$$

avec
$$q_k = (\alpha\beta) \cdot a_k$$
$$= \alpha\beta a_k.$$

Les deux résultats sont identiques : $p_k = q_k$. Donc :

[A'] $\quad (\forall \alpha)(\forall \beta)(\forall A) \qquad \alpha \cdot (\beta \cdot A) = (\alpha \cdot \beta) \cdot A.$

Associativité mixte de la loi externe et de la multiplication des polynômes.

Soient les polynômes :

$$A = (a_0 ; a_1 ; \dots ; a_i ; \dots)$$
$$B = (b_0 ; b_1 ; \dots ; b_j ; \dots)$$

et le scalaire $\alpha \cdot (\alpha \in K)$.

On a : $\alpha \cdot (AB) = (p_0 ; p_1 ; \ldots ; p_k ; \ldots)$

avec
$$p_k = \alpha \cdot \sum_{i+j=k} a_i b_j$$
$$= \sum_{i+j=k} \alpha a_i b_j$$

et $(\alpha A) \cdot B = (q_0 ; q_1 ; \ldots ; q_k ; \ldots)$

avec
$$q_k = \sum_{i+j=k} (\alpha a_i) \cdot b_j .$$
$$= \sum_{i+j=k} \alpha a_i b_j .$$

Les deux résultats sont identiques : $p_k = q_k$. Donc, en tenant compte de la commutativité :

[A″] $(\forall \alpha)(\forall A)(\forall B) : \quad \alpha \cdot (A \cdot B) = (\alpha A) \cdot B = A \cdot (\alpha \cdot B).$

445. Espace vectoriel (ou module des polynômes.)

1° On suppose que les polynômes sont construits sur un corps commutatif K.

L'ensemble $\mathcal{P}$ (K) est muni de deux lois :

Une addition qui possède les propriétés [A] [N] [S] [C].

Une loi externe (multiplication par un scalaire) qui possède la propriété [N′]

Les deux lois sont liées par les relations [A′] [D′] [D″].

En conséquence :

$\mathcal{P}$ (K) est un espace vectoriel sur le corps K.

2° On suppose que les polynômes sont construits sur un anneau commutatif unitaire A.

Les opérations sont les mêmes, et possèdent les mêmes propriétés; mais dans ce cas on dit que $\mathcal{P}$ est muni d'une structure de module.

Et :

$\mathcal{P}$ (A) est un module sur l'anneau A.

446. Anneau des polynômes.

On considère l'ensemble $\mathcal{P}$ (K) des polynômes construits sur un corps K ou sur un anneau K.

L'ensemble $\mathcal{P}$ (K) est muni de deux lois internes :

Une addition qui possède les propriétés [A] [N] [S] [C].

Une multiplication qui possède les propriétés [A] [N] [C]

Les deux lois sont liées par la relation [D].

Donc :

$\mathcal{P}$ (K) est un anneau commutatif unitaire.

447. Algèbre des polynômes.

L'ensemble $\mathcal{P}$ (K) est muni de deux lois internes et d'une loi externe :
Une addition qui possède les propriétés $\boxed{A}$ $\boxed{N}$ $\boxed{S}$ $\boxed{C}$.
Une multiplication qui possède les propriétés $\boxed{A}$ $\boxed{N}$ $\boxed{C}$.
Une multiplication par un scalaire qui possède la propriété $\boxed{N'}$.
Les trois lois sont liées par les relations $\boxed{A'}$ $\boxed{A''}$ $\boxed{D}$ $\boxed{D'}$ $\boxed{D''}$.

$\mathcal{P}$ (K) est donc à la fois un espace vectoriel (ou un module) et un anneau, avec en plus la relation $\boxed{A''}$; on dit que $\mathcal{P}$ (K) est un algèbre.

$\mathcal{P}$ (K) est un algèbre sur le corps K (ou l'anneau K).

448. Base de l'espace vectoriel des polynômes.

Soit le polynôme

$$A = (a_0; a_1; ...; a_n; 0; 0; ...)$$

Il s'écrit :

$$A = (a_0; 0; 0; ...) + (0; a_1; 0; 0; ...) + ... + (0; 0; ...; a_n; 0; 0; ...)$$
$$= a_0 \cdot (1; 0; 0; ...) + a_1 \cdot (0; 1; 0; 0; ...) + ... + a_n \cdot (0; ...; 1; 0; 0; ...)$$

On pose

$$e_0 = (1; 0; 0; ...)$$
$$e_1 = (0; 1; 0; ...)$$
$$...............$$
$$e_n = (0; 0; ...; 1; 0; 0; ...)$$

et alors :

$$A = a_0 \cdot e_0 + a_1 \cdot e_1 + ... + a_n \cdot e_n$$

Les polynômes $e_0; e_1; e_2 ...; e_n; ...$ sont linéairement indépendants.

L'ensemble $\mathcal{B}_0 = \{e_0; e_1; ...; e_n; ...\}$ constitue la base canonique de l'espace vectoriel $\mathcal{P}$. Un polynôme quelconque de $\mathcal{P}$ s'exprime par une combinaison des éléments de $\mathcal{B}_0$.

449. Propriétés des polynômes de la base canonique $\mathcal{B}_0$.

1° Soient les deux polynômes :

$$e_p = (\underbrace{0; 0; ...; 0}_{p \text{ zéros}}; 1; 0; 0; ...)$$

et

$$e_q = (\underbrace{0; 0; ...; 0}_{q \text{ zéros}}; 1; 0; 0; ...)$$

de la base $\mathcal{B}_0$.

Le produit $e_p \cdot e_q$ de ces deux polynômes peut se calculer à l'aide du tableau suivant

----	0	----------	1	0	0	----
0	0	----------	0	0	0	----
----	----	----------	----	----	----	----
1	0	----------	1	0	0	----
0	0	----------	0	0	0	----
0	0	----------	0	0	0	----
----	----	----------	----	----	----	----

On voit donc que :

$$e_p \cdot e_q = (\underbrace{0\,;0\,;\ldots\,;0}_{p+q \text{ zéros}}\,;1\,;0\,;0\,;\ldots)$$

D'où la formule :

$$\mathbf{e}_p \cdot \mathbf{e}_q = \mathbf{e}_{p+q}. \qquad (449\,;1)$$

2° On a :

$$A \cdot e_0 = A$$

Donc :

$$e_0 = 1. \qquad (449\,;2)$$

e_0 est le polynôme unité.

Par suite :

$$\begin{aligned} A &= (a_0\,;0\,;0\,;\ldots) \\ &= a_0 \cdot (1\,;0\,;0\,;\ldots) \\ &= a_0 \cdot 1. \\ &= a_0. \end{aligned}$$

Un polynôme tel que $A = (a_0; 0; 0; \ldots)$ est un « polynôme constant ». Autrement dit.

Les polynômes constants peuvent être identifiés aux éléments du corps K.

3° On pose :

$$e_1 = u \qquad (449\,;3)$$

D'où :

$$e_2 = e_1 \cdot e_1 = u^2$$
$$e_3 = e_2 \cdot e_1 = u^3$$
$$\dots\dots\dots\dots$$
$$e_n = u^n \qquad (449;4)$$
$$\dots\dots$$

Le polynôme u est appelé l'indéterminée.

Au lieu de noter $\mathcal{T}(K)$ on note souvent $K[u]$.

4º Avec cette nouvelle notation la base $\mathcal{B}_0$ est

$$\mathcal{B}_0 = \{ \mathbf{1}; \mathbf{u}; \mathbf{u}^2; \mathbf{u}^3; \dots; \mathbf{u}^n; \dots \} \qquad (449;5)$$

et le polynôme A s'écrit

$$\boldsymbol{A} = \mathbf{a}_0 + \mathbf{a}_1 \cdot \mathbf{u} + \mathbf{a}_2 \cdot \mathbf{u}^2 + \mathbf{a}_3 \cdot \mathbf{u}^3 + \dots + \mathbf{a}_n \cdot \mathbf{u}^n \qquad (449;6)$$

5º *Cette expression d'un polynôme est particulièrement commode dans les calculs sur les polynômes.*

Ainsi soient les polynômes :

$$A = (2; -1; 3; 0; 0; \dots)$$
$$= 2 - u + 3u^2$$

et

$$B = (-1; 4; 0; 0; \dots)$$
$$= -1 + 4u.$$

On a :

$$A + B = 2 - u + 3u^2 - 1 + 4u$$
$$= 1 + 3u + 3u^2$$
$$= (1; 3; 3; 0; 0; \dots)$$

et

$$A \cdot B = (2 - u + 3u^2)\ (-1 + 4u)$$
$$= -2 + u - 3u^2 + 8u - 4u^2 + 12u$$
$$= -2 + 9u - 7u^2 + 12u^3$$
$$= (-2; 9; -7; 12; 0; 0; \dots)$$

450. Intégrité.

On suppose maintenant que K est un anneau sans diviseur de 0 ou est un corps.

1º Soient deux polynômes :

$$A = (a_0; \dots; a_n; 0; 0; \dots)$$
$$B = (b_0; \dots; b_m; 0; 0; \dots)$$

Si a_n est le dernier coefficient non nul de A, et si b_m est le dernier coefficient non nul de B, le dernier coefficient de AB est $a_n b_m$. (Cf. nº 442). Comme K n'a pas de diviseur de 0, $a_n b_m$ n'est pas nul.

D'où l'implication

$$(A \neq 0 \quad \text{et} \quad B \neq 0) \Rightarrow (A \cdot B \neq 0).$$

2° Par contraposition :

$$(AB = 0) \Rightarrow (A = 0 \quad \text{ou} \quad B = 0).$$

Autrement dit :

Si K n'a pas de diviseur de zéro, K[u] est un anneau intègre.

451. Régularité.

Tous les éléments de $\mathcal{P}^* = \mathcal{P} - \{0\}$ sont réguliers par rapport à la multiplication.

En effet, si A, P, Q sont des polynômes, avec $A \neq 0$, on a :

$$A \cdot P = A \cdot Q \Rightarrow AP - AQ = 0 \Rightarrow A(P - Q) = 0$$

Puisque A n'est pas nul, d'après l'intégrité, on a $P - Q = 0$ ou $P = Q$.

Et :

$$(A \neq 0 \quad \text{et} \quad AP = AQ) \Rightarrow (P = Q).$$

452. Degré d'un polynôme.

1° Soit le polynôme :

$$A = (a_0; a_1; \ldots; a_n; 0; 0 \ldots)$$

dans lequel le dernier coefficient non nul est a_n.

On dit alors que le degré de A est n.

On note :

$$\deg A = n.$$

Il faut remarquer que le rang de a_n est $n + 1$.

On a aussi :

$$A = a_0 + a_1 u + a_2 \cdot u^2 + \ldots + a_n \cdot u^n$$

Le degré est donc l'exposant le plus grand des puissances de l'indéterminée u.

2° Soient les deux polynômes A, B et leur somme A + B.

Alors :

$$\begin{aligned}
\deg A > \deg B &\Rightarrow \deg(A + B) = \deg A \\
\deg A = \deg B &\Rightarrow \deg(A + B) \leqslant (\deg A = \deg B) \\
\deg A < \deg B &\Rightarrow \deg(A + B) = \deg B.
\end{aligned}$$

3° Soient les deux polynômes *non nuls* A, B et leur produit A·B.

Alors :

$$\mathbf{deg}\ AB = \mathbf{deg}\ A + \mathbf{deg}\ B.$$

4° *Le degré d'un « polynôme constant » non nul est 0.*
Le degré du polynôme nul est indéterminé.

453. Division euclidienne des polynômes sur un corps.

On suppose maintenant que K est un corps.

1° Soient deux polynômes A et B de $\mathcal{I} = K[u]$.

On considère l'ensemble des polynômes :

$$E = \{ A - BX / X \in \mathcal{I} \}.$$

Lorsque X décrit l'ensemble $\mathcal{I}$ des polynômes, le degré de A — BX varie. Le degré de A — BX étant un entier naturel, ***il existe un polynôme Q, au moins, tel que***

$$(\forall X)(X \in \mathcal{I}) : \quad \mathbf{deg}(A - BX) \geqslant \mathbf{deg}(A - B \cdot Q) \quad (453;1)$$

On a :

$$m = \deg(A - BQ) = \operatorname*{Inf}_{X \in \mathcal{I}}[\deg(A - BX)] \qquad (453;2)$$

2° On se propose de démontrer l'inégalité stricte :

$$\mathbf{deg}(A - BQ) < \mathbf{deg}\, B. \qquad (453;3)$$

Soient :

$$A = a_0 + a_1 \cdot u + \ldots + a_n\ u^n$$
$$B = b_0 + b_1 \cdot u + \ldots + b_p\ u^p$$
$$A - BQ = c_0 + c_1 \cdot u + \ldots + c_m\ u^m$$

c_m n'est pas nul puisque le degré de A — BQ est m.

Pour démontrer la formule (453; 3) on fait une réduction à l'absurde; et on suppose deg B ⩾ deg *(A — BQ), c'est-à-dire* m ⩾ p.

En multipliant B par $\frac{c_m}{b_p} u^{m-p}$ on a :

$$\frac{c_m}{b_p} B \cdot u^{m-p} = \frac{b_0 c_m}{b_p} u^{m-p} + \frac{b_1 c_m}{b_p} u^{m-p+1} + \cdots + \frac{c_m}{b_p} b_{p-1} \cdot u^{m-1} + c_m \cdot u^m.$$

D'où :

$$A - BQ - \frac{c_m}{b_p} Bu^{m-p} = A - B\left(Q + \frac{c_m}{b_p} \cdot u^{m-p}\right)$$
$$= (c_0 + c_1 \cdot u + \dots + c_m u^m) - \left(\frac{b_0 c_m}{b_p} u^{m-p} + \dots + c_m u^m\right)$$
$$= c_0 + \dots + c_{m-1}u^{m-1} - \frac{b_0 c_m}{b_p} u^{m-p} - \frac{c_m}{b_p} b_{p-1}u^{m-1}$$
$$= c_0 + \dots + \left(c_{m-1} - \frac{c_m b_{p-1}}{b_p}\right) u^{m-1}.$$

Alors avec $Q_1 = Q + \frac{c_m}{b_p} u^{m-p}$ on aurait :

$$A - BQ_1 = c_0 + \dots + \left(c_{m-1} - \frac{c_m b_{p-1}}{b_p}\right) u^{m-1}$$

et

$$\deg(A - BQ_1) \leqslant m - 1.$$

Ce qui est contraire au résultat (453; 2). Donc: $m < p$ ou

$$\deg (A - BQ) < \deg B.$$

3° On se propose maintenant de démontrer l'unicité du polynôme Q. On suppose qu'il existe un second polynôme Q′ tel que

$$\deg (A - BQ') = m.$$

On a donc, d'après 2° :

$$\deg (A - BQ') < \deg B \qquad (453; 4)$$

En supposant Q′ différent de Q, donc :

$$Q' - Q \neq 0$$

On a :

$$\deg(Q' - Q) \geqslant 0$$

et par suite

$$\deg B(Q' - Q) \geqslant \deg B \qquad (453; 5)$$

D'autre part :

$$(A - BQ) - (A - BQ') = B (Q' - Q)$$

Des relations (453; 3), (453; 4) on déduit :

$$\deg [(A - BQ) - (A - BQ'] < \deg B$$

ou

$$\deg B (Q' - Q) < \deg B \qquad (453; 6)$$

Les résultats (453; 5) et (453; 6) sont contradictoires donc $Q' = Q$.

4° On peut alors énoncer :

Etant donné deux polynômes non nuls A et B, il existe un polynôme non nul et un seul tel que

$$A - BQ = 0$$

ou tel que

$$(\forall X)(X \in \mathcal{T}) \quad \deg(A - BQ) < \deg(A - BX)$$

avec de plus

$$\deg(A - BQ) < \deg B.$$

5° On pose :

$$A - BQ = R.$$

Q est le quotient et R est le reste de la division euclidienne de A par B.

On a donc :

$$A = BQ + R \quad \textit{avec} \quad \deg R < \deg B.$$

◇ *Exemple 1.*

Diviser $A = u^3 + 2u^2 - 3u - 6$ *par* $B = u + 2$.

L'opération se dispose de la façon suivante, à la manière des divisions numériques :

$$\begin{array}{r|l} u^3 + 2u^2 - 3u - 6 & u + 2 \\ \cline{2-2} -u^3 - 2u^2 \phantom{{}- 3u - 6} & u^2 - 3 \\ \cline{1-1} 0 \phantom{{}- 3u - 6} & \\ +3u + 6 & \\ \cline{1-1} 0 & \end{array}$$

Donc :

$$u^3 + 2u^2 - 3u - 6 = (u + 2)(u^2 - 3).$$

◇ *Exemple 2.*

Diviser $A = u^4 - 3u^3 - 5u^2 + 3u - 5$ par B $u^2 - u - 1$.

On a :

$$\begin{array}{r|l} u_4 - 3u^3 - 5u^2 + 3u - 5 & u^2 - u - 1 \\ \cline{2-2} -u_4 + u^3 + u^2 \phantom{{}+ 3u - 5} & u^2 - 2u - 6 \\ \cline{1-1} -2u^3 - 4u^2 \phantom{{}+ 3u - 5} & \\ +2u^3 - 2u^2 - 2u \phantom{{}- 5} & \\ \cline{1-1} -6u^2 + u \phantom{{}- 5} & \\ +6u^2 - 6u - 6 & \\ \cline{1-1} -5u - 11 & \end{array}$$

Donc :

$$u_4 - 3u^3 - 5u^2 + 3u - 5 \equiv (u^2 - u - 1)(u^2 - 2u - 6) - (5u + 11).$$

454. Polynômes premiers sur K.

Soit l'algèbre $K[u]$, K étant un corps.

1° ***Un polynôme A est dit réductible sur K, s'il existe deux polynômes A_1 et A_2 de $K[u]$ tels que $A = A_1 \cdot A_2$, avec deg $A_1 \neq 0$ et deg $A_2 \neq 0$.***

◇ *Exemple.*

Soit le polynôme $A = u^2 - 3$. On a :

$$A = (u - \sqrt{3})(u + \sqrt{3})$$

Donc A est réductible dans K = R.

2° ***Lorsqu'un polynôme A n'est pas réductible sur K, il est dit irréductible sur K, ou premier sur K.***

◇ *Exemple.*

Soit le polynôme $A = u^2 + 1$. Il est irréductible sur R, mais il est réductible sur C.

En effet :

$$\begin{aligned} A &= u^2 + 1 \\ &= u^2 - (-1) \\ &= u^2 - i^2 \\ &= (u + i)(u - i). \end{aligned}$$

455. P.G.C.D. et P.P.C.M.

A partir de la notion de polynômes premiers, il est possible de construire une théorie du P.G.C.D. et une théorie du P.P.C.M. de deux polynômes à une indéterminée. L'étude de ces théories est réservée pour une classe ultérieure.

CHAPITRE XXXIV

POLYNOMES FORMELS A PLUSIEURS INDÉTERMINÉES

456. Polynômes formels sur un anneau ou sur un corps, à deux indéterminées.

Dans ce qui suit K désigne un anneau commutatif unitaire ou un corps commutatif.

On appelle polynôme à deux indéterminées une suite infinie à deux indices d'éléments de K telle qu'à partir d'un certain élément tous les éléments de la suite sont nuls.

Un élément de la suite se note donc $a_{k;l}$. Les éléments $a_{k;l}$ sont les coefficients du polynôme.

On peut disposer les coefficients d'un polynôme à deux indéterminées dans un tableau à double entrée :

$a_{0;0}$	$a_{1;0}$	$a_{2;0}$	--------	$a_{n;0}$	0	0	----
$a_{0;1}$	$a_{1;1}$	$a_{2;1}$	--------	$a_{n;1}$	0	0	----
$a_{0;2}$	$a_{1;2}$	$a_{2;2}$	--------	$a_{n;2}$	0	0	----
----	----	----	--------	----	----	----	----
$a_{0;m}$	$a_{1;m}$	$a_{2;m}$	--------	$a_{n;m}$	0	0	----
0	0	0	--------	0	0	0	----
0	0	0	--------	0	0	0	----

Si le coefficient envisagé est $a_{k;l}$, il est situé à l'intersection de la colonne notée k et de la ligne notée l.

457. Polynômes identiques ou égaux.

Deux polynômes A et B sont identiques, ou égaux, s'ils ont les mêmes coefficients.

Donc : $$(A = B) \Leftrightarrow ((\forall i)(\forall j)\ a_{i;j} = b_{i;j}).$$

458. Addition des polynômes à deux indéterminées.

Soient les polynômes à deux indéterminées A et B.

On appelle somme des polynômes A et B, le polynôme $S = A + B$, ***dont le coefficient général est*** $S_{k;l} = a_{k;l} + b_{k;l}$.

◇ *Exemple. Soient les deux polynômes*

$A =$

-1	4	2	0	
0	1	6	0	
4	3	0	0	
0	0	0	0	

et $B =$

0	2	5	0	
-1	1	9	0	
4	3	0	0	
0	0	0	0	

Calculer $S = A + B$.

On a immédiatement :

$S = A + B =$

-1	6	7	0
-1	2	15	0
8	6	0	0
0	0	0	0

459. Propriétés de l'addition.

L'addition des polynômes à deux indéterminées possède les propriétés suivantes :

Commutativité.

On a :

[C] $$(\forall A)(\forall B) \quad A + B = B + A.$$

En effet :

$$(\forall k)(\forall l) \quad a_{k;l} + b_{k;l} = b_{k;l} + a_{k;l}.$$

Associativité.

On a :

[A] $$(\forall A)(\forall B)(\forall C) \quad (A + B) + C = A + (B + C).$$

En effet :

$$(\forall k)(\forall l) : \quad (a_{k;l} + b_{k;l}) + c_{k;l} = a_{k;l} + (b_{k;l} + c_{k;l}).$$

Existence d'un polynôme neutre pour l'addition.

Le polynôme E dont tous les éléments sont nuls est neutre pour l'addition :

[N] $$(\exists E)(\forall A) \quad A + E = E + A = A.$$

En effet :

$$(\forall k)(\forall l) \quad a_{k;l} + 0 = 0 + a_{k;l} = a_{k;l}$$

La loi étant additive, on note E = 0; et

$$(\forall A) \quad A + 0 = 0 + A = A.$$

L'ensemble des polynômes est symétrisé pour l'addition.

Soit le polynôme A, de coefficient général $a_{k;l}$. Le polynôme A' de coefficient général $-a_{k;l}$ est symétrique de A pour l'addition :

[S] $$(\forall A)(\exists A') \quad A + A' = A' + A = 0.$$

En effet :

$$(\forall k)(\forall l) \quad a_{k;l} + (-a_{k;l}) = (-a_{k;l}) + a_{k;l} = 0.$$

$A' = -A$ est le polynôme opposé du polynôme A.

460. Groupe additif.

1° ***L'ensemble des polynômes à deux indéterminées, muni de la loi d'addition est groupe additif commutatif***

2° On en déduit, comme au n° 438 :

Tous les polynômes sont réguliers pour l'addition.

3° Comme au n° 439, on peut alors définir une *soustraction*.

461. Multiplication d'un polynôme par un scalaire.

Soient un scalaire λ ($\lambda \in K$) et un polynôme A de coefficient général $a_{k;l}$.

On appelle produit du polynôme A par le nombre λ le polynôme P dont le coefficient général est $p_{k;l} = \lambda \cdot a_{k;l}$.

Cette multiplication est donc une loi externe.

462. Propriété de la multiplication d'un polynôme par un scalaire.

On a :

N' $$(\forall A) \qquad 1 \cdot A = A.$$

En effet :

$$(\forall k)(\forall l) \qquad 1 \cdot a_{k;l} = a_{k;l}.$$

463. Multiplication des polynômes.

Soient les polynômes A et B de coefficients généraux respectifs $a_{k;l}$ et $b_{k;l}$.

On appelle produit du polynôme A par le polynôme B le polynôme Π dont le coefficient général est

$$\pi_{i;j} = \sum_{\substack{k+p=i \\ l+q=j}} (a_{k;l} \cdot b_{p;q})$$

Donc :

$$\pi_{0;0} = a_{0;0} \cdot b_{0,0}$$
$$\pi_{1;0} = a_{1;0} \cdot b_{0;0} + a_{0;0} \cdot b_{1;0}$$
$$\pi_{0;1} = a_{0;0} \cdot b_{0;1} + a_{0;1} \cdot b_{0;0}$$
$$\pi_{1;1} = a_{1;1} \cdot b_{0;0} + a_{1;0} \cdot b_{0;1} + a_{0;1} \cdot b_{1;0} + a_{0;0} \cdot b_{1.1}$$

....

464. Propriétés de la multiplication.

La multiplication des polynômes à deux indéterminées possède les propriétés suivantes :

Commutativité.

On a :

C $\quad (\forall A)(\forall B) \qquad A \cdot B = B \cdot A.$

En effet, le coefficient général $\pi_{i;j}$ du produit AB est :

$$\pi_{i;j} = \sum_{\substack{k+p=i \\ l+q=j}} (a_{k;l} \cdot b_{p;q})$$

et le coefficient général $\pi'_{i;j}$ du produit AB est :

$$\pi'_{i;j} = \sum_{\substack{p+k=i \\ p+q=j}} (b_{p;q} \cdot a_{k;l}) = \sum_{\substack{k+p=i \\ l+q=j}} (a_{k;l} \cdot b_{p;q})$$

On a bien :

$$\pi'_{i;j} = \pi_{i;j}$$

Associativité.

On a :

A $\quad (\forall A)(\forall B)(\forall C) \qquad (A \cdot B) \cdot C = A \cdot (B \cdot C).$

En effet, le coefficient général $\Pi_{r;s}$ du produit (AB) C est

$$\pi_{r;s} = \sum_{\substack{i+\lambda=r \\ j+\mu=s}} \left[\left(\sum_{\substack{k+p=i \\ l+q=j}} a_{k;l} \cdot b_{p;q} \right) \cdot c_{\lambda;\mu} \right] = \sum_{\substack{k+p+\lambda=r \\ l+q+\mu=s}} (a_{k;l} b_{p;q} c_{\lambda;\mu})$$

et le coefficient général $\Pi_{r;s}$ du produit A · (BC) est

$$\pi'_{r;s} = \sum_{\substack{k+m=r \\ l+n=s}} \left[a_{k;l} \cdot \sum_{\substack{p+\lambda=m \\ q+\mu=n}} \left(b_{p;q} c_{\lambda;\mu} \right) \right] = \sum_{\substack{k+p+\lambda=r \\ l+q+\mu=s}} (a_{k;l} \cdot b_{p;q} \cdot c_{\lambda;\mu}).$$

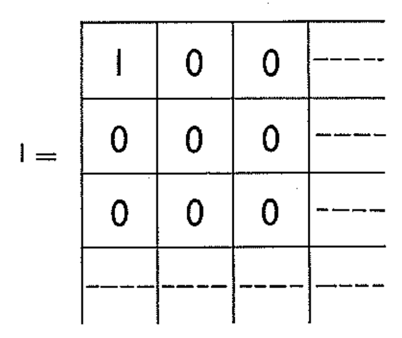
On a bien :

$$\pi'_{r;s} = \pi_{r;s}$$

Existence d'un polynôme neutre pour la multiplication.

Soit le polynôme A de coefficient général $a_{k;l}$.

On envisage le polynôme I dont le coefficient $I_{0;0}$ est 1, et dont tous les autres coefficients sont nuls.



I	0	0	----
0	0	0	----
0	0	0	----
----	----	----	----

On a :

[N] $(\forall A) \quad A \cdot I = I \cdot A = A.$

En effet :

$$\pi_{i;j} = \sum_{\substack{k+p=i \\ l+q=j}} I_{k;l} \cdot a_{p;q}$$
$$= I_{0;0} \cdot a_{i;j}$$
$$= 1 \times a_{i;j}$$
$$= a_{i;j}$$

465. Relations entre les diverses lois.

Distributivité de la multiplication pour l'addition.

On a :

[D] $(\forall A)(\forall B)(\forall M) \qquad M(A + B) = M \cdot A + M \cdot B.$

En effet, le coefficient général $\Pi_{i;j}$ de M (A + B) est :

$$\pi_{i;j} = \sum_{\substack{k+p=i \\ l+q=j}} m_{k;l} (a_{p;q} + b_{p;q})$$
$$= \sum_{\substack{k+p=i \\ l+q=j}} (m_{k;l} \cdot a_{p;q}) + \sum_{\substack{k+p=i \\ l+q=j}} (m_{k;l} \cdot b_{p;q})$$

et le coefficient général $\Pi'_{i;j}$ de MA + MB est :

$$\pi'_{i;j} = \sum_{\substack{k+p=i \\ l+q=j}} (m_{k;l} \cdot a_{p;q}) + \sum_{\substack{k+p=i \\ l+q=j}} (m_{k;l} \cdot b_{p;q}).$$

On a bien :

$$\pi'_{i;j} = \pi_{i;j}$$

Distributivité de la loi externe pour l'addition des polynômes.

On a :

D' $(\forall\alpha)(\forall A)(\forall B) \quad \alpha \cdot (A + B) = \alpha \cdot A + \alpha \cdot B.$

En effet, le coefficient général $\Pi_{i;j}$ de α (A + B) est :

$$\pi_{i;j} = \alpha(a_{i;j} + b_{i;j})$$

et le coefficient général $\pi'_{i;j}$ de αA + αB est :

$$\pi'_{i;j} = \alpha \cdot a_{i;j} + \alpha \cdot b_{i;j}$$

On a bien :

$$\pi'_{i;j} = \pi_{i;j}$$

Distributivité de la loi externe pour l'addition dans K.

On a :

D'' $(\forall\alpha)(\forall\beta)(\forall A) \quad (\alpha + \beta) A = \alpha \cdot A + \beta \cdot A.$

En effet, le coefficient général $\pi_{i;j}$ de $(\alpha + \beta) \cdot$ A est :

$$\pi_{i;j} = (\alpha + \beta) \cdot a_{i;j}$$

et le coefficient général $\pi'_{i;j}$ de αA + βA est :

$$\begin{aligned}\pi'_{i;j} &= \alpha \cdot a_{i;j} + \beta \cdot a_{i;j} \\ &= (\alpha + \beta) a_{i;j}\end{aligned}$$

On a bien :

$$\pi'_{i;j} = \pi_{i;j}$$

Associativité mixte de la loi externe et de la multiplication des scalaires.

On a :

A' $(\forall\alpha)(\forall\beta)(\forall A) \quad \alpha . (\beta \cdot A) = (\alpha \cdot \beta) \cdot A.$

En effet, le coefffcient général $\pi_{i;j}$ de $\alpha(\beta$A) est :

$$\begin{aligned}\pi_{i;j} &= \alpha \cdot (\beta \cdot a_{i;j}) \\ &= \alpha \cdot \beta \cdot a_{i;j}\end{aligned}$$

et le coefficient général $\pi'_{i;j}$ de $(\alpha\beta)$ A est :

$$\begin{aligned}\pi'_{i;j} &= (\alpha\beta)\, a_{i;j} \\ &= \alpha\beta a_{i;j}\end{aligned}$$

On a bien :

$$\pi'_{i;j} = \pi_{i;j}$$

Associativité mixte de la loi externe et de la multiplication des polynômes.

On a :

[A″] $(\forall\alpha)(\forall A)(\forall B) \qquad \alpha\cdot(A\cdot B) = (\alpha\cdot A)\cdot B = A\cdot(\alpha B).$

En effet, le coefficient général $\pi_{i;j}$ de $\alpha(AB)$ est :

$$\pi_{i;j} = \alpha \cdot \sum_{\substack{k+p=i\\l+q=j}} a_{k;l} \cdot b_{p;q}$$

$$= \sum_{\substack{k+p=i\\l+q=j}} \alpha a_{k;l} b_{p;q}$$

Le coefficient général $\pi'_{i;j}$ de $(\alpha A)\cdot B$ est :

$$\pi'_{i;j} = \sum_{\substack{k+p=i\\l+q=j}} (\alpha a_{k;l}\, b_{p;q})$$

$$= \sum_{\substack{k+p=i\\l+q=j}} (\alpha a_{k;l} b_{p;q})$$

et le coefficient général $\pi''_{i;j}$ de $A\cdot(\alpha B)$ est :

$$\pi''_{i;j} = \sum_{\substack{k+p=i\\l+q=j}} a_{kl} \cdot (\alpha b_{p;q})$$

$$= \sum_{\substack{k+p=i\\l+q=j}} \alpha a_{k;l} b_{p;q}$$

466. Espace vectoriel (ou module) des polynômes à deux indéterminées.

Dans l'ensemble $\mathcal{P}$ des polynômes à deux indéterminées on a introduit :
Une addition possédant les propriétés [A] [N] [S] [C] ;
Une multiplication par un scalaire possédant la propriété [N′]
Ces deux lois sont liées par les relations [A′] [D′] [D″].
En conséquence,

Si K est un corps, l'ensemble des polynômes à deux indéterminées est un espace vectoriel sur le corps K.

Si K est un anneau, l'ensemble des polynômes à deux indéterminées est un module sur l'anneau K.

467. Anneau des polynômes à deux indéterminées.

L'ensemble $\mathcal{P}$ des polynômes à deux indéterminées a été muni de deux lois internes :

Une addition possédant les propriétés [A] [N] [S] [C];
Une multiplication possédant les propriétés [A] [N] [C].
Ces deux lois sont liées par la relation [D].

Donc :

L'ensemble des polynômes à deux indéterminées est un anneau commutatif unitaire.

468. Algèbre des polynômes à deux indéterminées.

L'ensemble $\mathcal{P}$ des polynômes à deux indéterminées a été muni de deux lois internes et d'une loi externe :

Une addition possédant les propriétés [A] [N] [S] [C];
Une multiplication possédant les propriétés [A] [N] [C];
Une multiplication par un scalaire possédant la propriété [N'].
Ces trois lois sont liées par les relations [A'] [A''] [D] [D'] [D''].

Donc :

L'ensemble des polynômes à deux indéterminées est une algèbre.

469. Base de l'espace vectoriel des polynômes à deux indéterminées.

1° On désigne par $e_{i;j}$ le polynôme à deux indéterminées dans lequel tous les coefficients sont nuls sauf le coefficient $a_{i;j}$ qui est égal à 1.

2° Le polynôme $e_{0;0}$ est tel que $e_{0;0}\,A = A$. C'est le polynôme unité $I_{0;0}$ envisagé au n° 464.

3° En appliquant la définition de la multiplication des polynômes, on a:

$$e_{k;l} \cdot e_{p;q} = e_{k+p;l+q}. \qquad (469\,;\,1)$$

En posant alors :

$$e_{0;0} = 1 \qquad e_{1;0} = u \qquad e_{0;1} = v$$

on a : (469; 2)

$$e_{k;l} = u^k \cdot v^l.$$

Les polynômes u et v *sont les deux indéterminées.*

4° Un polynôme A s'écrit :

$$A = a_{0;0} \cdot e_{0;0} + a_{1;0} \cdot e_{1;0} + a_{0;1} \cdot e_{0;1} + \dots + a_{k;l} \cdot e_{k;l} + \dots + a_{m;n} \cdot e_{m;n}$$

ou

$$A = a_{0;0} + a_{1;0} \cdot u + a_{0;1} \cdot v + \dots + a_{k;l} u^k v^l + \dots + a_{m;n} \cdot u^m v^n \qquad (469\,;\,3)$$

Aussi on désigne l'ensemble $\mathcal{P}$ des polynômes sur K à deux indéterminées par K [u; v]

$$\mathcal{P} = K\,[u;\,v].$$

5° La forme (469; 3) est particulièrement commode dans les calculs sur les polynômes.

◇ *Exemple.*

Soient $A = 1 + u - v$ *et* $B = 2 - v - u^2$. *Calculer* $A + B$ *et* AB.

On a :

$$A + B = 1 + u - v + 2 - v - u^2$$
$$= 3 + u - 2v - u^2.$$

Et :

$$AB = (1 + u - v)(2 - v + u^2)$$
$$= 2 - v + u^2 + 2u - uv + u^3 - 2v + v^2 - u^2v$$
$$= 2 + 2u - 3v + u^2 - uv + v^2 + u^3 - u^2v.$$

470. Généralisation.

On peut étendre la définition et l'étude précédente des polynômes à deux indéterminées à l'étude des polynômes à plus de deux indéterminées.

Les résultats sont analogues.

CHAPITRE XXXV

FRACTIONS DE POLYNÔMES

471. Relation d'équivalence dans $\mathcal{P} \times \mathcal{P}^*$.

On considère dans ce chapitre l'anneau $\mathcal{P} = K[u]$ des polynômes à une indéterminée construits sur le corps commutatif K. On pose $\mathcal{P}^* = \mathcal{P} - \{0\}$.

1° Soient $\alpha = (A; B)$ et $\alpha' = (A'; B')$ deux éléments de l'ensemble-produit $\mathcal{P} \times \mathcal{P}^*$.

Ces deux éléments $\alpha = (A; B)$ et $\alpha' = (A'; B')$ sont dits liés par la relation $\mathcal{R}$ si $AB' = BA'$.

On note alors :

$$\alpha \mathcal{R} \alpha'$$

ou

$$\alpha = \alpha', \text{ mod } \mathcal{R}$$

ou

$$(A ; B) = (A' ; B'), \text{ mod } \mathcal{R}$$

Et :

$$[(A ; B) = (A' ; B'), \text{ mod } \mathcal{R}] \iff [AB' = BA'].$$

2° La relation $\mathcal{R}$ ainsi définie est une relation d'équivalence; en effet, elle est : *réflexive :*

$$(A; B) = (A; B), \text{ mod } \mathcal{R}, \quad \text{car } AB = BA$$

Donc :

$\boxed{R}$ $$\alpha = \alpha, \text{ mod } \mathcal{R}.$$

symétrique :

$$\begin{aligned}(A ; B) = (A' ; B'), \text{ mod } \mathcal{R} &\iff AB' = BA' \\ &\iff A'B = B'A \\ &\iff (A' ; B') = (A ; B), \text{ mod } \mathcal{R}.\end{aligned}$$

Donc :

$\boxed{S}$ $$(\alpha = \alpha', \text{ mod } \mathcal{R}) \Rightarrow (\alpha' = \alpha, \text{ mod } \mathcal{R}).$$

transitive :

$$\left.\begin{array}{l}(A;B)=(A';B'),\ \text{mod}\ \mathcal{R}\\ \text{et}\\ (A';B')=(A'';B''),\ \text{mod}\ \mathcal{R}\end{array}\right\}\Rightarrow\left\{\begin{array}{l}AB'=BA'\\ \text{et}\\ A'B''=B'A''\end{array}\right\}\Rightarrow AB'A'B''=BA'B'A''$$

$$\Rightarrow AB''=BA''$$

$$\Rightarrow (A;B)=(A'';B''),\ \text{mod}\ \mathcal{R}.$$

On a simplifié $AB'A'B'' = BA'B'A''$, par $A'B'$. B' n'est pas nul, donc est régulier pour la multiplication. La démonstration précédente suppose donc que A' n'est pas nul. Lorsque A' est nul, $AB' = BA'$ implique $A = 0$, et $A'B'' = B'A''$ implique $A'' = 0$. Les trois éléments α, α', α'' envisagés sont alors

$$\alpha = (0;\ B) \qquad \alpha' = (0;\ B') \qquad \alpha'' = (0;\ B'')$$

et ils sont deux à deux équivalents.

Donc :

[T] $(\alpha = \alpha',\ \text{mod}\ \mathcal{R}\ \text{ et }\ \alpha' = \alpha'',\ \text{mod}\ \mathcal{R}) \Rightarrow (\alpha = \alpha'',\ \text{mod}\ \mathcal{R})$.

3° Soit l'élément $\alpha = (A;\ B)$. Le polynôme A est le numérateur; le polynôme B est le dénominateur.

On note :

$$\alpha = \frac{A}{B}.$$

Par exemple :

$$\alpha = \frac{1 + u + u^2}{1 - u^2 - u^3}.$$

4° Les éléments $(A;\ B)$ et $(PA;\ PB)$ où $P \in \mathcal{P}^*$ sont équivalents.

En effet, on a :

$$A \cdot PB = B \cdot PA$$

472. Classes d'équivalence.

La relation d'équivalence précédente $\mathcal{R}$ partage l'ensemble $\mathcal{P} \times \mathcal{P}^*$ en classes d'équivalence.

Les classes d'équivalence sont des fractions de polynômes à une indéterminée.

L'ensemble des fractions de polynômes à une indéterminée est désigné par $\mathcal{F}$.

Donc :

$$\mathcal{F} = \frac{\mathcal{P} \times \mathcal{P}^*}{\mathcal{R}}.$$

473. Formes réduites.

Une classe d'équivalence est définie par l'un quelconque des couples (A; B) de cette classe.

Si $A = \Delta \cdot A_1$ et $B = \Delta \cdot B_1$, on a :

$$AB' = BA' \Rightarrow \Delta \cdot A_1 B' = \Delta \cdot B_1 A'$$
$$\Rightarrow A_1 \cdot B' = B_1 \cdot A'$$

Donc : $$(A; B) = (A'; B') = (A_1; B_1).$$

$(A_1; B_1)$ est une forme simplifiée de la fraction.
Si Δ est le P.G.C.D. des polynômes A et B, $(A_1; B_1)$ est la forme réduite de la fraction.

474. Réduction au même dénominateur.

Deux fractions de polynômes sont réduites au même dénominateur si leurs dénominateurs sont égaux.

Lorsqu'on veut réduire plusieurs fractions de polynômes au même dénominateur il y a souvent intérêt à prendre comme dénominateur commun le P.P.C.M. des dénominateurs.

◇ *Exemple.*

Soient les fractions :

$$F = \frac{4u + 1}{3u - 1} \qquad G = \frac{4u - 1}{3u + 1}.$$

Les réduire au même dénominateur.

Le P.P.C.M. des polynômes $3u - 1$ et $3u + 1$ est le produit $9u^2 - 1$ de ces deux polynômes.

Donc : $$F = \frac{(4u + 1)(3u + 1)}{9u^2 - 1} = \frac{12u^2 + 7u + 1}{9u^2 - 1}$$

et

$$G = \frac{(4u - 1)(3u - 1)}{9u^2 - 1} = \frac{12u^2 - 7u + 1}{9u^2 - 1}.$$

475. Addition des éléments de $\mathcal{F} \times \mathcal{F}^*$.

Soient $\alpha = (A; B)$ et $\alpha' = (A'; B')$ deux éléments $\mathcal{F} \times \mathcal{F}^*$. On définit l'addition par la formule

$$\alpha + \alpha' = \frac{A}{B} + \frac{A'}{B'}$$
$$= \frac{AB' + BA'}{BB'}.$$

476. Compatibilité de l'équivalence et de l'addition.

Soient les éléments $\alpha = (A ; B) = \frac{A}{B}, \alpha' = (A' ; B') = \frac{A'}{B'}$ et leur somme $\alpha + \alpha' = (AB' + BA' ; BB') = \frac{AB' + BA'}{BB'}$.

Soient les éléments $\beta = (C ; D) = \frac{C}{D}, \beta' = (C' ; D') = \frac{C'}{D'}$ et leur somme $\beta + \beta' = (CD' + DC' ; DD') = \frac{CD' + DC'}{DD'}$.

On se propose de démontrer l'implication :

$$(\alpha = \beta; \textbf{mod } \mathcal{R} \textbf{ et } \alpha' = \beta', \textbf{mod } \mathcal{R}) \Rightarrow (\alpha + \alpha' = \beta + \beta', \textbf{mod } \mathcal{R})$$

En effet :

$$(\alpha = \beta;\ \text{mod } \mathcal{R}) \Rightarrow AD = BC \quad \text{ou} \quad AD - BC = 0$$

et

$$(\alpha'; \beta';\ \text{mod } \mathcal{R}) \Rightarrow A'D' = B'C' \quad \text{ou} \quad A'D' - B'C' = 0$$

D'où :

$$B'D' (AD - BC) + BD (A'D' - B'C') = 0$$

ou
$$ADB'D' - BCB'D' + BDA'D' - BDB'C' = 0$$

ou
$$DD' (AB' + BA') = BB' (CD' + DC')$$

ou

$$\frac{AB' + BA'}{BB'} = \frac{CD' + DC'}{DD'}$$

ou
$$\alpha + \alpha' = \beta + \beta', \text{ mod } \mathcal{R}.$$

477. Addition des fractions de polynômes.

Le résultat précédent montre que pour additionner deux fractions de polynômes, on peut prendre un élément quelconque des classes d'équivalence.

En particulier, on peut réduire les éléments au même dénominateur μ. On obtient alors la règle classique :

$$\frac{a}{\mu} + \frac{a'}{\mu} = \frac{a + a'}{\mu}.$$

◇ *Exemple.*

Soient les fractions :

$$F = \frac{4u + 1}{3u - 1}, \qquad G = \frac{4u - 1}{3u + 1}.$$

Calculer $F + G$.

On a :

$$F + G = \frac{4u+1}{3u-1} + \frac{4u-1}{3u+1}$$
$$= \frac{12u^2+7u+1}{9u^2-1} + \frac{12u^2-7u+1}{9u^2-1}$$
$$= \frac{24u^2+2}{9u^2-1}$$
$$= \frac{2(12u^2+1)}{9u^2-1}.$$

478. Propriétés de l'addition.

L'addition des fractions de polynômes possède les propriétés suivantes :

Commutativité.

On a :

$$\alpha + \alpha' = \frac{A}{D} + \frac{A'}{D}$$
$$= \frac{A + A'}{D}$$

et

$$\alpha' + \alpha = \frac{A'}{D} + \frac{A}{D}$$
$$= \frac{A' + A}{D}.$$

Les deux résultats sont identiques; donc :

[C] $(\forall\alpha)(\forall\alpha') \quad \alpha + \alpha' = \alpha' + \alpha.$

Associativité.

On a :

$$(\alpha + \alpha') + \alpha'' = \left(\frac{A}{D} + \frac{A'}{D}\right) + \frac{A''}{D}$$
$$= \frac{A + A'}{D} + \frac{A''}{D}$$
$$= \frac{A + A' + A''}{D}$$

et

$$\alpha + (\alpha' + \alpha'') = \frac{A}{D} + \left(\frac{A'}{D} + \frac{A''}{D}\right)$$
$$= \frac{A}{D} + \frac{A' + A''}{D}$$
$$= \frac{A + A' + A''}{D}.$$

Les deux résultats sont identiques; donc:

$\boxed{A}$ $(\forall\alpha)(\forall\alpha')(\forall\alpha'')\quad (\alpha + \alpha') + \alpha'' = \alpha + (\alpha' + \alpha'').$

Existence d'un élément neutre pour l'addition.

Soit :

$$e = (0;1) = (0;2) = \ldots = (0;D) = \ldots$$

On a :

$$\alpha + e = \frac{A}{D} + \frac{0}{D}$$
$$= \frac{A+0}{D}$$
$$= \frac{A}{D}$$
$$= \alpha.$$

En tenant compte de la commutativité, on a:

$\boxed{N}$ $(\exists e)(\forall\alpha)\quad \alpha + e = e + \alpha = \alpha.$

La loi étant additive, on note: $e = 0$; et

$$(\forall\alpha)\quad \alpha + \boldsymbol{0} = \boldsymbol{0} + \alpha = \alpha.$$

L'ensemble des fractions est symétrisé pour l'addition.

Soit la fraction :

$$\alpha = (A;B) = \frac{A}{B}.$$

On considère la fraction:

$$\alpha' = (-A;B) = \frac{-A}{B}.$$

On a :

$$\alpha + \alpha' = \frac{A}{B} + \frac{-A}{B}$$
$$= \frac{A + (-A)}{B}$$
$$= \frac{0}{B}$$
$$= 0.$$

En tenant compte de la commutativité :

[S] $(\forall\alpha)(\exists\alpha') \quad \alpha + \alpha' = \alpha' + \alpha = 0.$

On note $\alpha' := -\alpha$; $-\alpha$ est l'opposé de α.

479. Groupe additif.

L'ensemble $\mathcal{F}$ des fractions de polynômes à une indéterminée a été muni d'une addition qui possède les propriétés [A] [N] [S] [C].

Donc :

L'ensemble $\mathcal{F}$ des fractions de polynômes à une indéterminée est un groupe additif commutatif.

On pose :

$$\mathcal{F}^* = \mathcal{F} - \{0\}.$$

480. Régularité.

Soient :

$$\alpha \in \mathcal{F}; \quad \beta \in \mathcal{F}; \quad \mu \in \mathcal{F}.$$

On suppose que l'on a :

$$\alpha + \mu = \beta + \mu.$$

En ajoutant $-\mu$ aux deux membres de cette égalité on obtient :

$$(\alpha + \mu) + (-\mu) = (\beta + \mu) + (-\mu)$$

ou

$$\alpha + [\mu + (-\mu)] = \beta + [\mu + (-\mu)]$$

ou

$$\alpha + 0 = \beta + 0$$

ou

$$\alpha = \beta.$$

Donc :

$$(\forall\alpha)(\forall\beta)(\forall\mu) : \quad \alpha + \mu = \beta + \mu \Rightarrow \alpha = \beta.$$

Et :

Toutes les fractions sont régulières pour l'addition.

481. Soustraction.

Soient $\alpha \in \mathcal{F}$ et $\beta \in \mathcal{F}$. Trouver $x \in \mathcal{F}$ telle que

$$\alpha = \beta + x$$

s'appelle soustraire β de α.

En ajoutant $-\beta$ aux deux membres de l'égalité, on a :

$$\begin{aligned}\alpha + (-\beta) &= (\beta + x) + (-\beta)\\ &= x + [\beta + (-\beta)]\\ &= x + 0\\ &= x.\end{aligned}$$

La fraction cherchée est donc :

$$x = \alpha + (-\beta).$$

Pour soustraire une fraction on ajoute son opposée.

La fraction x est la différence entre α et β. On le note :

$$x = \alpha - \beta.$$

On a donc :

$$\alpha - \beta = \alpha + (-\beta).$$

482. Multiplication des éléments de $\mathcal{I} \times \mathcal{I}^*$.

Soient $\alpha = (A; B)$ et $\alpha' = (A'; B')$ deux éléments de $\mathcal{I} \times \mathcal{I}^*$. On définit la multiplication par la formule

$$\alpha \cdot \alpha' = \frac{A}{B} \times \frac{A'}{B'} = \frac{AA'}{BB'}.$$

483. Comptabilité de l'équivalence et de la multiplication.

Soient les éléments $\alpha = \frac{A}{B}$, $\alpha' = \frac{A'}{B'}$ et leur produit $\alpha\alpha' = \frac{AA'}{BB'}$.

Soient les éléments $\beta = \frac{C}{D}$, $\beta' = \frac{C'}{D'}$ et leur produit $\beta\beta' = \frac{CC'}{DD'}$.

On se propose de démontrer l'implication :

$$(\alpha = \beta,\ \textbf{mod}\ \mathfrak{R}\ \textbf{et}\ \alpha' = \beta',\ \textbf{mod}\ \mathfrak{R}) \Rightarrow (\alpha \cdot \alpha' = \beta \cdot \beta',\ \textbf{mod}\ \mathfrak{R}).$$

En effet :

$$(\alpha = \beta, \text{ mod } \mathfrak{R}) \Rightarrow AD = BC$$

et

$$(\alpha' = \beta', \text{ mod } \mathfrak{R}) \Rightarrow A'D' = B'C'.$$

D'où, par multiplication :

$$AA' \cdot DD' = BB' \cdot CC'$$

ou

$$\frac{AA'}{BB'} = \frac{CC'}{DD'}$$

ou

$$\alpha \cdot \alpha' = \beta \cdot \beta', \text{ mod } \mathfrak{R}.$$

484. Multiplication des fractions de polynômes.

Le résultat précédent montre que pour multiplier deux fractions de polynômes, on peut prendre un élément quelconque des classes d'équivalence.

◇ *Exemple.*

Soient les fractions :

$$F = \frac{u+1}{u-1} \qquad \text{et} \qquad G = \frac{u-1}{u^2-1}.$$

Calculer FG.

On a :

$$\begin{aligned} F \cdot G &= \frac{u+1}{u-1} \cdot \frac{u-1}{(u+1)(u-1)} \\ &= \frac{(u+1)(u-1)}{(u-1)(u+1)(u-1)} \\ &= \frac{1}{u-1}. \end{aligned}$$

485. Propriétés de la multiplication.

La multiplication des fractions de polynômes possède les propriétés suivantes :

Commutativité.

On a :

$$\begin{aligned} \alpha \cdot \alpha' &= \frac{A}{B} \cdot \frac{A'}{B'} \\ &= \frac{AA'}{BB'} \end{aligned}$$

et

$$\begin{aligned} \alpha' \cdot \alpha &= \frac{A'}{B'} \cdot \frac{A}{B} \\ &= \frac{A' \cdot A}{B' \cdot B}. \end{aligned}$$

Les deux résultats sont identiques ; donc :

[C] $$(\forall \alpha)(\forall \alpha') \qquad \alpha \cdot \alpha' = \alpha' \cdot \alpha.$$

Associativité.

On a :

$$(\alpha \cdot \alpha') \cdot \alpha'' = \frac{AA'}{BB'} \cdot \frac{A''}{B''}$$
$$= \frac{AA'A''}{BB'B''}$$

et

$$\alpha \cdot (\alpha' \cdot \alpha'') = \frac{A}{B} \cdot \frac{A'A''}{B'B''}$$
$$= \frac{AA'A''}{BB'B''}.$$

Les deux résultats sont identiques ; donc :

[A] $(\forall\alpha)(\forall\alpha')(\forall\alpha'') \qquad (\alpha \cdot \alpha') \cdot \alpha'' = \alpha \cdot (\alpha' \cdot \alpha'').$

Existence d'un élément neutre pour la multiplication.

Soit e = (1; 1), 1 étant le polynôme neutre pour la multiplication.

On a :

$$\alpha \cdot e = \frac{A}{B} \times \frac{1}{1}$$
$$= \frac{A}{B}$$
$$= \alpha.$$

En tenant compte de la commutativité, on a :

[N] $(\exists e)(\forall\alpha) \qquad \alpha \cdot e = e \cdot \alpha = \alpha.$

La loi étant multiplicative, on note : e = 1; et

$$(\forall\alpha) \qquad \alpha \cdot 1 = 1 \cdot \alpha = \alpha.$$

L'ensemble des fractions est symétrisé pour la multiplication.

Soit la fraction non nulle : $(A \neq 0)$

$$\alpha = \frac{A}{B}.$$

On considère la fraction :

$$\alpha' = \frac{B}{A}.$$

On a :

$$\alpha \cdot \alpha' = \frac{A}{B} \times \frac{B}{A}$$
$$= \frac{A \cdot B}{B \cdot A}$$
$$= 1.$$

En tenant compte de la commutativité, on a :

S $$(\forall\alpha)(\exists\alpha') : \quad \alpha \cdot \alpha' = \alpha' \cdot \alpha = 1.$$

Donc :

Toutes les fractions de $\mathcal{F}$ sont symétrisées pour la multiplication.

On pose : $\alpha' = \dfrac{1}{\alpha} = \alpha^{-1}$

486. Groupe multiplicatif.

On considère l'ensemble $\mathcal{F}^* = \mathcal{F} - \{0\}$ muni de la loi de multiplication précédente. Ces lois possèdent les propriétés A N S C. Donc :

Les fractions de polynômes non nulles forment un groupe multiplicatif commutatif.

487. Régularité.

Soient :

$$\alpha \in \mathcal{F}; \quad \beta \in \mathcal{F}; \quad \mu \in \mathcal{F}^*.$$

On suppose que l'on a :

$$\alpha \cdot \mu = \beta \cdot \mu.$$

En multiplant par $\dfrac{1}{\mu}$ les deux membres de cette égalité, on obtient

$$(\alpha \cdot \mu) \cdot \frac{1}{\mu} = (\beta \cdot \mu) \cdot \frac{1}{\mu}$$

ou

$$\alpha \cdot \left(\mu \times \frac{1}{\mu}\right) = \beta \cdot \left(\mu \cdot \frac{1}{\mu}\right)$$

ou

$$\alpha \cdot 1 = \beta \cdot 1$$

ou

$$\alpha = \beta.$$

Donc :

$$(\forall\alpha)(\forall\beta)(\forall\mu)(\mu \in \mathcal{F}^*) : \quad \alpha \cdot \mu = \beta \cdot \mu \Rightarrow \alpha = \beta.$$

Et :

Toutes les fractions non nulles sont régulières pour la multiplication.

488. Division.

Soient** $\alpha \in \mathcal{F}$ **et** $\beta \in \mathcal{F}^*$. **Trouver** $x \in \mathcal{F}$ **telle que

$$\alpha = \beta \cdot x$$

***s'appelle diviser** α **par** β.*

En multipliant par $\frac{1}{\beta}$ les deux membres de l'égalité, on a :

$$\begin{aligned} \alpha \times \frac{1}{\beta} &= (\beta \cdot x)\frac{1}{\beta} \\ &= x \cdot \left(\beta \cdot \frac{1}{\beta}\right) \\ &= x \cdot 1 \\ &= x. \end{aligned}$$

La fraction cherchée est donc :

$$x = \alpha \cdot \frac{1}{\beta}.$$

Pour diviser par une fraction non nulle on multiplie par son inverse.

489. Distributivité de la multiplication pour l'addition.

Soient les fractions de polynômes :

$$\alpha = \frac{A}{D}, \qquad \alpha' = \frac{A'}{D} \qquad \text{et} \qquad \mu = \frac{P}{Q}.$$

On a :

$$\begin{aligned} \mu \cdot (\alpha + \alpha') &= \frac{P}{Q} \cdot \frac{A + A'}{D} \\ &= \frac{P(A + A')}{Q \cdot D} \end{aligned}$$

et

$$\begin{aligned} \mu \cdot \alpha + \mu \cdot \alpha' &= \frac{P \cdot A}{Q \cdot D} + \frac{P \cdot A'}{Q \cdot D} \\ &= \frac{PA + PA'}{Q \cdot D} \\ &= \frac{P(A + A')}{Q \cdot D}. \end{aligned}$$

Les deux résultats sont identiques, et :

[D] $(\forall \alpha)(\forall \alpha')(\forall \mu) : \quad \mu(\alpha + \alpha') = \mu\alpha + \mu\alpha'.$

Donc :

La multiplication des fractions de polynômes est distributive pour l'addition.

490. Le corps $\mathcal{F}$ des fractions de polynômes.

L'ensemble $\mathcal{F}$ des fractions de polynômes à une indéterminée est muni de deux lois internes :

Une addition qui possède les propriétés $\boxed{A}$ $\boxed{N}$ $\boxed{S}$ $\boxed{C}$.

Une multiplication qui possède les propriétés $\boxed{A}$ $\boxed{N}$ $\boxed{S}$ $\boxed{C}$.

Ces deux lois sont liées par la relation $\boxed{D}$.

Donc :

$\mathcal{F}$ est le corps des fractions de polynômes à une indéterminée.

491. Algèbre des fractions de polynômes.

On peut définir une loi externe.

Soient $\lambda \in K$ et $\alpha \in \mathcal{F}$.

On définit la loi externe par la formule

$$\lambda \cdot \alpha = \lambda \cdot \frac{A}{B} = \frac{\lambda A}{B}.$$

On montre alors facilement que

$\mathcal{F}$ est une algèbre sur le corps K.

492. Suite de rapports égaux.

Une fraction $\frac{A}{B}$ de nombres ou de polynômes est encore appelée un rapport, le rapport de A à B.

On considère une suite de rapport égaux :

$$\frac{A'}{A} = \frac{B'}{B} = \frac{C'}{C} = k$$

k désignant un nombre (rationnel, réel, complexe) ou une fraction de polynômes.

On a immédiatement :

$$A' = k \cdot A$$
$$B' = k \cdot B$$
$$C' = k \cdot C$$

En multipliant les égalités précédentes par α, β, γ respectivement, on obtient :

$$\alpha A' = k \cdot \alpha A$$
$$\beta B' = k \cdot \beta B$$
$$\gamma C' = k \cdot \gamma C$$

D'où par addition :

$$\alpha A' + \beta B' + \gamma C' = k(\alpha A + \beta B + \gamma C)$$

et encore si $\alpha A + \beta B + \gamma C \neq 0$:

$$k = \frac{\alpha A' + \beta B' + \gamma C'}{\alpha A + \beta B + \gamma C}.$$

Finalement :

$$\frac{\boldsymbol{A'}}{\boldsymbol{A}} = \frac{\boldsymbol{B'}}{\boldsymbol{B}} = \frac{\boldsymbol{C'}}{\boldsymbol{C}} = \frac{\alpha \boldsymbol{A'} + \beta \boldsymbol{B'} + \gamma \boldsymbol{C'}}{\alpha \boldsymbol{A} + \beta \boldsymbol{B} + \gamma \boldsymbol{C}}.$$

CHAPITRE XXXVI

AXIOMATISATION

493. Remarque préliminaire.

Après la lecture de cette première partie du cours une remarque importante s'impose. De nombreuses démonstrations sont analogues et paraissent pratiquement identiques. Il est alors normal de les analyser et de rechercher les raisons de cette analogie. Cette recherche mène directement à la notion d'axiomatique.

494. La notion de groupe.

Dans ce qui précède, la notion de groupe est apparue de nombreuses fois :

Groupe additif dans Z (cf. n° 186).
Groupe additif dans Q (cf. n° 242).
Groupe multiplicatif dans Q* (cf. n° 249).
Groupe additif dans Z/p (cf. n° 216).
Groupe multiplicatif dans $(Z/p)^*$, p premier (cf. n° 223).
Groupe additif dans R (cf. n° 283).
Groupe multiplicatif dans R* (cf. n° 300).
Groupe additif dans C (cf. n° 326).
Groupe multiplicatif dans C* (cf. n° 331).
Groupe additif dans l'espace vectoriel K^n (cf. n° 354).
Groupe additif dans l'espace vectoriel M_1^n (cf. n° 366).
Groupe additif des polynômes à une indéterminée (cf. n° 437).
Groupe additif des polynômes à deux indéterminées (cf. n° 460).
Groupe additif des fractions de polynômes (cf. n° 479).
Groupe multiplicatif des fractions de polynômes (cf. n° 486).

Quelles sont les propriétés qui, chaque fois, ont caractérisé le groupe? Ce sont essentiellement les trois propriétés suivantes, appelées *axiomes* du groupe. Si la loi interne est notée $*$ ce sont :

L'axiome d'associativité :

[A] $(\forall x)(\forall y)(\forall z) \quad (x * y) * z = x * (y * z).$

L'axiome d'existence d'un neutre:

N $(\exists e)(\forall x) \quad x \ast e = e \ast x = x.$

L'axiome de symétrisation

S $(\forall x)(\exists x') \quad x \ast x' = x' \ast x = e.$

Si de plus la loi $\ast$ est commutative, c'est-à-dire si elle vérifie *l'axiome de commutativité*

C $(\forall x)(\forall y) \quad x \ast y = y \ast x,$

on dit que le groupe est commutatif ou abélien.

Le groupe est souvent noté G ou $\{ G; \ast \}$.

495. Unicité du neutre dans un groupe.

Soit un groupe $\{ G; \ast \}$.

S'il existe deux éléments neutres e et e' on a :
puisque e est neutre :

$$(\forall x) \quad x \ast e = e \ast x = x \qquad (495; 1)$$

et puisque e' est neutre :

$$(\forall x) \quad x \ast e' = e' \ast x = x. \qquad (495; 2)$$

En prenant $x = e'$ dans (495; 1), il vient :

$$e' \ast e = e \ast e' = e' \qquad (495; 3)$$

et en prenant $x = e$ dans (495; 2), il vient :

$$e \ast e' = e' \ast e = e. \qquad (495; 4)$$

En comparant (495; 3) et (495; 4), on obtient :

$$e = e'$$

Donc :

Dans un groupe le neutre est unique.

Remarque.

La démonstration précédente exige seulement l'axiome N.

Donc :

Si une loi interne possède un neutre, ce neutre est unique.

496. Unicité du symétrique dans un groupe.

Soit un groupe $\{ G ; \ast \}$; e est le neutre de ce groupe.
On considère un élément quelconque x du groupe.

Si x possédait deux symétriques x' et x'' on aurait, en utilisant l'axiome [A] :

$$x'' \ast (x \ast x') = (x'' \ast x) \ast x'$$

ou, puisque $x \ast x' = e$ et $x'' \ast x = e$:

$$x'' \ast e = e \ast x'$$

ou

$$x'' = x'.$$

Donc :

Dans un groupe un élément quelconque a un symétrique unique.

497. Régularité dans un groupe.

En se reportant aux 15 groupes examinés dans ce premier volume, on remarque que chaque fois on a démontré que tous les éléments du groupe étaient réguliers à gauche, c'est-à-dire que tous les éléments du groupe possèdent la propriété suivante :

$[R_G]$ $(\forall m)(\forall x)(\forall y) \quad m \ast x = m \ast y \Rightarrow x = y.$

D'ailleurs tous les groupes étudiés étant commutatifs, la régularité à droite s'en déduit :

$[R_D]$ $(\forall m)(\forall x)(\forall y) \quad x \ast m = y \ast m \Rightarrow x = y.$

Cette régularité dépend-elle des exemples de groupes présentés? ou bien dépend-elle uniquement des trois axiomes du groupe?

Pour s'en rendre compte il suffit de comparer les 15 démonstrations; l'analogie est frappante. La nature de l'opération utilisée, addition ou multiplication, n'intervient pas dans les démonstrations, mais seules les propriétés [A] [N] [S] sont utilisées.

Il doit alors être possible de donner une démonstration indépendante des éléments utilisés et de l'opération utilisée.

Soit donc un groupe $\{ G ; \ast \}$, c'est-à-dire un ensemble d'éléments ***non précisés,*** $G = \{ x ; y ; z ; \ldots \}$, muni d'une loi de composition interne, notée $\ast$, ***non précisée,*** mais satisfaisant aux trois axiomes [A] [N] [S].

On peut montrer que tous les éléments de G sont réguliers, à droite et à gauche.

En effet, puisque l'axiome [S] est vérifié, il existe m' tel que $m \ast m' = m' \ast m = e$, e étant le neutre du groupe (axiome [N]). Alors, on a :

$$m' \ast (m \ast x) = m' \ast (m \ast y)$$

ou, en utilisant l'associativité (axiome [A]) :

$$(m' * m) * x = (m' * m) * y,$$

ou, en utilisant l'axiome [S] :

$$e * x = e * y$$

ou, en utilisant l'axiome [N] :

$$x = y.$$

Finalement :

[R_G] $\quad (\forall m)(\forall x)(\forall y) \quad m * x = m * y \Rightarrow x = y.$

La démonstration précédente utilise *uniquement* les axiomes [A] [N] [S], et ces trois axiomes sont tous utilisés. Il y a régularité à gauche ; on démontre de même la régularité à droite. On a donc [R] = { [R_G]; [R_D] } :

Dans un groupe, tous les éléments sont réguliers.

498. Utilité de l'axiomatisation.

En supposant que G est un groupe, on a démontré (cf. nº 495; 496; 497) les trois propriétés suivantes :

— le neutre e de G est unique;
— le symétrique x' de tout élément x de G est unique;
— tous les éléments de G sont réguliers.

La nature des éléments de G n'a pas été précisée, non plus que la nature de l'opération $*$; aussi chaque fois qu'un ensemble Γ sera muni d'une loi interne T possédant les propriétés [A] [N] [S], c'est-à-dire que $(\Gamma; T)$ sera un groupe, on pourra conclure sans aucune démonstration que :

— le neutre de Γ est unique;
— le symétrique x' de tout élément x de Γ pour la loi T est unique;
— tous les éléments de Γ sont réguliers pour la loi T.

Ainsi, dans Z, après avoir montré que l'addition possède les propriétés [A] [N] [S] [C] c'est-à-dire que { Z; + } est un groupe commutatif, on déduira, par exemple, sans démonstration que tous les éléments de Z sont réguliers pour l'addition.

Ainsi, dans Q*, après avoir montré que la multiplication possède les propriétés [A] [N] [S] [C], c'est-à-dire que { Q*; $*$ } est un groupe commutatif, on déduira sans démonstration que tous les éléments de Q* sont réguliers pour la multiplication.

Cela conduit à exposer une théorie des groupes, dans laquelle à partir des axiomes [A] [N] [S] on démontre des propriétés vraies dans tous les groupes particuliers.

On dit qu'on a axiomatisé la notion de groupe, ou qu'on a fait une axiomatique du groupe.

A un certain niveau des Mathématiques l'axiomatisation s'impose donc; et elle réalise une « économie de pensée » très importante, puisque déjà ici on donne une démonstration au lieu de quinze.

499. Opération inverse de l'opération du groupe.

Dans les 15 groupes étudiés, pour chaque groupe l'étude des propriétés a toujours comporté une soustraction si le groupe est additif, et une division si le groupe est multiplicatif. La soustraction est l'opération inverse (ou opposée) de l'addition, et la division est l'opération inverse de la multiplication.

Il est possible d'axiomatiser.

Soit un groupe $\{G; \ast\}$.

Etant donnés deux éléments a et b de G, on se propose de chercher l'élément x de G tel que

$$\mathbf{a \ast x = b}$$

a' désignant le symétrique de a, on a :

$$a' \ast (a \ast x) = a' \ast b$$

ou (associativité)

$$(a' \ast a) \ast x = a' \ast b$$

ou

$$e \ast x = a' \ast b$$

et

$$x = a' \ast b. \qquad (499;1)$$

De même on peut chercher l'élément y de G tel que

$$y \ast a = b.$$

On a :

$$(y \ast a) \ast a' = b \ast a'$$

ou

$$y \ast (a \ast a') = b \ast a'$$

ou

$$y \ast e = b \ast a'$$

et

$$y = b \ast a' \qquad (499;2)$$

Les éléments x et y ne sont égaux que si les éléments a' et b commutent; cela se produit en particulier si le groupe G est commutatif.

500. La notion d'anneau.

Plusieurs anneaux ont déjà été étudiés dans ce cours; il est donc utile de rappeler ici les propriétés caractéristiques d'un anneau, c'est-à-dire les axiomes de cet anneau.

Soit un ensemble A d'éléments x, y, z ..., muni de deux lois internes. Pour simplifier, la première loi est presque toujours notée additivement, et la seconde multiplicativement.

A ou $\{ A; +; \times \}$ est un anneau si les axiomes suivants sont vérifiés.

Addition. L'addition fait de A un groupe commutatif; elle possède donc les propriétés :

$\boxed{A}$ $(\forall x)(\forall y)(\forall z)$ $(x + y) + z = x + (y + z)$.

$\boxed{N}$ $(\exists e)(\forall x)$ $x + e = e + x = x$.

$\boxed{S}$ $(\forall x)(\exists x')$ $x + x' = x' + x = e$.

$\boxed{C}$ $(\forall x)(\forall y)$ $x + y = y + x$.

Le neutre e est noté 0; c'est l'élément nul ou le *zéro de l'anneau*; il est unique.

Le symétrique x' de x est noté $x' = -x$; c'est *l'opposé* de x; il est unique.

Multiplication. La multiplication est associative :

$\boxed{A}$ $(\forall x)(\forall y)(\forall z)$ $x \times (y \cdot z) = (x \cdot y) \cdot z$.

Relation entre les deux lois. La multiplication est distributive pour l'addition.

$\boxed{D}$ $\begin{cases} \boxed{D_g} & (\forall m)(\forall x)(\forall y) \quad m \cdot (x + y) = m \cdot x + m \cdot y. \\ \boxed{D_d} & (\forall m)(\forall x)(\forall y) \quad (x + y) \cdot m = x \cdot m + y \cdot m. \end{cases}$

Si ces 6 axiomes $\boxed{A}$ $\boxed{N}$ $\boxed{S}$ $\boxed{C}$, $\boxed{A}$, $\boxed{D}$ sont vérifiés, $\{ A; +; \times \}$ est un anneau.

Il peut arriver que la multiplication vérifie de plus l'un des deux axiomes suivants ou les deux :

$\boxed{N}$ $(\exists \varepsilon)(\forall x)$ $x \cdot \varepsilon = \varepsilon \cdot x = x$.

$\boxed{C}$ $(\forall x)(\forall y)$ $x \cdot y = y \cdot x$.

Si $\boxed{N}$ est vérifié, l'anneau est un *anneau unitaire*; ε est l'unité de cet anneau; il est unique (cf. n° 495, Remarque). On note en général $\varepsilon = 1$.

Si $\boxed{C}$ est vérifié, l'anneau est un *anneau commutatif.*

Ainsi, Z, Z/6 sont des anneaux unitaires commutatifs.

501. Diviseurs de zéro. Anneau intègre.

1° Dans l'anneau commutatif unitaire A = Z/6, on a vu que

$$\dot{2} \times \dot{3} = \dot{0} \quad \text{et} \quad \dot{3} \times \dot{4} = \dot{0}.$$

Ainsi le produit de deux éléments non nuls de A = Z/6 peut être nul. Dans l'anneau A = Z/6 les éléments $\dot{2}$, $\dot{3}$; $\dot{4}$ sont appelés des diviseurs de zéro.

Donc :

Dans un anneau, deux éléments non nuls a et b sont des diviseurs de zéro si leur produit est nul.

2° ***Un anneau A est intègre s'il n'a pas de diviseurs de zéro.***

La multiplication est intègre, c'est-à-dire possède la propriété d'*intégrité* :

$$\begin{cases} (\forall a)(\forall b) & (a \neq 0 \quad \text{et} \quad ab = 0) \Rightarrow (b = 0). \\ (\forall a)(\forall b) & (b \neq 0 \quad \text{et} \quad ab = 0) \Rightarrow (a = 0). \end{cases}$$

502. Régularité dans un anneau intègre.

Soit A un anneau intègre. On note A* = A − { 0 }. Il est possible de montrer que

Dans un anneau intègre tous les éléments de A* sont réguliers pour la multiplication.

Soient x et y des éléments de A, et m un élément de A* ($m \neq 0$).

On a :

$$(m \cdot x = m \cdot y) \Rightarrow (m \cdot x - m \cdot y = 0) \Rightarrow (m\,(x - y) = 0)$$
$$\Rightarrow (x - y = 0) \Rightarrow x = y$$

Ainsi :

[RG] $(\forall m)(m \in A^*), (\forall x)(\forall y) : \quad m \cdot x = m \cdot y \Rightarrow x = y.$

On démontre de même la régularité à droite.

503. La notion de corps.

Plusieurs corps ont été étudiés dans ce cours; il est donc utile de rappeler les axiomes du corps.

Soit un ensemble K d'éléments x, y, z ..., muni de deux lois internes, une addition et une multiplication.

K ou { K; +; × } est un corps si les axiomes suivants sont vérifiés.

Addition. L'addition fait de K un groupe commutatif; elle possède les propriétés :

[A] $(\forall x)(\forall y)(\forall z)$ $(x + y) + z = x + (y + z)$.

[N] $(\exists e)(\forall x)$ $x + e = e + x = x$.

[S] $(\forall x)(\exists x')$ $x + x' = x' + x = e$.

[C] $(\forall x)(\forall y)$ $x + y = y + x$.

Le neutre e est noté 0; c'est le zéro du corps; il est unique.

On pose $K^* = K - \{0\}$.

$x' = -x$ est l'opposé de x; il est unique.

Multiplication. La multiplication dans K* vérifie les axiomes d'un groupe.

[A] $(\forall x)(\forall y)(\forall z)$ $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

[N] $(\exists \varepsilon)(\forall x)$ $x \cdot \varepsilon = \varepsilon \cdot x = x$.

[S] $(\forall x)(\exists x')$ $x \cdot x' = x' \cdot x = \varepsilon$.

Le neutre ε est noté 1; c'est l'unité du corps; il est unique.
Le symétrique x' de x pour la multiplication est noté $x' = x^{-1}$; c'est l'inverse de x; il est unique.

Relation entre les deux lois. La multiplication est distributive pour l'addition :

[D] $\begin{cases} [D_G] & (\forall m)(\forall x)(\forall y) \quad m \cdot (x + y) = m \cdot x + m \cdot y. \\ [D_D] & (\forall m)(\forall x)(\forall y) \quad (x + y) \cdot m = x \cdot m + y \cdot m. \end{cases}$

Si ces 8 axiomes [A] [N] [S] [C]; [A] [N] [S]; [D] sont vérifiés, $\{K; +; *\}$ est un corps.

Il peut arriver que la multiplication dans K* vérifie de plus l'axiome suivant :

[C] $(\forall x)(\forall y)$ $x \cdot y = y \cdot x$.

Dans ce cas le corps est un corps commutatif.
Ainsi, Q, R, C sont des corps commutatifs.

504. Espaces vectoriels. Modules.

Plusieurs espaces vectoriels ont été étudiés dans ce cours.

Soient un ensemble E d'éléments $E = \{X; Y; Z \ldots\}$ et un anneau commutatif unitaire $\Omega = A$ ou un corps commutatif $\Omega = K$, $\Omega = \{\alpha; \beta; \ldots\}$.
E est muni d'une loi interne notée additivement et d'une loi externe notée .

E ou $\{E; \Omega; +; \cdot\}$ vérifie les axiomes suivants :

Addition. L'addition fait de E un groupe commutatif; elle possède les propriétés :

[A] $(\forall X)(\forall Y)(\forall Z)$ $(X + Y) + Z = X + (Y + Z)$.

[N] $(\exists e)(\forall X)$ $X + e = e + X = X$.

[S] · $(\forall X)(\exists X')$ $X + X' = X' + X = e$.

[C] $(\forall X)(\forall Y)$ $X + Y = Y + X$.

Le neutre e est noté 0. Il est unique.
X' est noté $- X$; c'est l'opposé de X; il est unique.

Multiplication par un scalaire. Ω est un anneau commutatif unitaire ou un corps commutatif; soit ε l'unité de Ω; on le note $\varepsilon = 1$. Les éléments de Ω sont des scalaires ou des opérateurs.

La multiplication par un scalaire possède la propriété :

[N'] $(\forall X)$ $1 \cdot X = X$.

Relation entre deux lois. La loi interne et la loi externe sont liées par des relations de distributivité et d'associativité mixte :

[D'] $(\forall \alpha)(\forall X)(\forall Y)$ $\alpha \cdot (X + Y) = \alpha \cdot X + \alpha \cdot Y$.

[D''] $(\forall \alpha)(\forall \beta)(\forall X)$ $(\alpha + \beta) \cdot X = \alpha \cdot X + \beta \cdot X$.

[A'] $(\forall \alpha)(\forall \beta)(\forall X)$ $\alpha \cdot (\beta X) = (\alpha\beta) \cdot X$.

Si $\Omega = A$ est un anneau commutatif unitaire $\{E; A; +; \cdot\}$ est un module sur l'anneau A.

Si $\Omega = K$ est un corps commutatif $\{E; K; +; \cdot\}$ est un espace vectoriel sur le corps K.

Ainsi $\mathcal{M}_1^3$ et K^2 sont des espaces vectoriels sur R (ou C, ou K).

Dans R on peut considérer la multiplication comme une loi externe : $E = R$ et $\Omega = R$. Donc :

R est un espace vectoriel sur R, de dimension 1.

De même :

C est un espace vectoriel sur C, de dimension 1.

De plus, un nombre complexe $z \in C$ s'écrit $z = x \cdot 1 + y \cdot i$ avec $x \in R$ et $y \in R$. Donc C est un espace vectoriel sur R, et la dimension de C est 2, puisque $\{1; i\}$ est la base canonique de C.

C est un espace vectoriel sur R, de dimension 2.

505. La notion d'algèbre.

Quelques algèbres ont été rencontrées dans ce cours.

Soient un ensemble $E = \{x; y; z; ...\}$ *et un anneau commutatif unitaire* $\Omega = A$ *ou un corps commutatif* $\Omega = K : \Omega = \{\alpha; \beta; ...\}$.

E est muni de deux lois internes, une addition et une multiplication, et d'une loi externe. Ces lois vérifient les axiomes suivants :

Addition. L'addition fait de E un groupe commutatif; elle possède les propriétés :

[A] $(\forall x)(\forall y)(\forall z)$ $(x + y) + z = x + (y + z)$.

[N] $(\exists e)(\forall x)$ $x + e = e + x = x$. $(e = 0)$

[S] $(\forall x)(\exists x')$ $x + x' = x' + x = e$. $(x' = -x)$

[C] $(\forall x)(\forall y)$ $x + y = y + x$.

Multiplication. La multiplication dans E possède la propriété suivante :

[A] $(\forall x)(\forall y)(\forall z)$ $(x \cdot y)\, z = x\,(y \cdot z)$.

Multiplication par un scalaire. La multiplication possède la propriété :

[N'] $(\forall x)$ $1 \cdot x = x$.

Relation entre les trois lois. Les deux lois internes et la loi externe sont liées par des relations de distributivités et d'associativités mixtes.

[D] { [D$_g$] $(\forall m)(\forall x)(\forall y)$ $m \cdot (x + y) = m \cdot x + m \cdot y$.
[D$_d$] $(\forall m)(\forall x)(\forall y)$ $(x + y) \cdot m = x \cdot m + y \cdot m$.

[D'] $(\forall \alpha)(\forall x)(\forall y)$ $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$.

[D''] $(\forall \alpha)(\forall \beta)(\forall x)$ $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$.

[A'] $(\forall \alpha)(\forall \beta)(\forall x)$ $\alpha \cdot (\beta \cdot x) = (\alpha\beta) \cdot x$.

[A''] $(\forall \alpha)(\forall x)(\forall y)$ $\alpha \cdot (x \cdot y) = (\alpha \cdot x) \cdot y = x \cdot (\alpha \cdot y)$.

Si ces 11 axiomes sont vérifiés, E est une algèbre sur l'anneau A ou sur le corps K.

Généralement la multiplication possède un élément neutre et est commutative :

[N] $(\exists\varepsilon)(\forall x)$ $x \cdot \varepsilon = \varepsilon \cdot x = x$ $(\varepsilon = 1)$

[C] $(\forall x)(\forall y)$ $x \cdot y = y \cdot x.$

L'algèbre E est alors unitaire et commutative.

Une algèbre est donc un anneau et un *module* vérifiant en plus l'axiome [A''].

Ainsi K[u] et K[u; v] sont des algèbres commutatives.

R et C peuvent être considérés comme des algèbres.

506. Structures algébriques.

Lorsqu'un ensemble E est muni d'une loi ou de plusieurs lois qui en font un groupe, ou un anneau, ou un corps, ou un module, ou un espace vectoriel, ou une algèbre, on dit que E est muni d'une structure algébrique.

La théorie de ces structures est axiomatisée. L'étude de ces axiomatiques est réservée pour une classe ultérieure; elle a été abordée pour les groupes et les anneaux.

507. Produits scalaires.

Dans ce cours, un seul produit scalaire a été rencontré : le produit scalaire euclidien. Il y a beaucoup d'autres produits scalaires; on a donc été amené, pour réaliser une économie de pensée, à axiomatiser la notion de produit scalaire.

On envisage *un espace vectoriel sur le corps R* et une application f de E × E dans R :

$$f : \quad (X ; Y) \in E \times E \longrightarrow f(X ; Y) \in R.$$

L'application f *est un* ***produit scalaire réel*** *si elle vérifie les axiomes suivants :*

[S₁] $(\forall X_1)(\forall X_2)(\forall Y)$ $f(X_1 + X_2 ; Y) = f(X_1 ; Y) + f(X_2 ; Y).$

[S₂] $(\forall \lambda)(\forall X)(\forall Y)$ $f(\lambda X ; Y) = \lambda \cdot f(X ; Y).$

[S₃] $(\forall X)(\forall Y)$ $f(X ; Y) = f(Y ; X).$

[S₄] $(\forall X)$ $f(X ; X) > 0$ *si* $X \in E^*.$

Ainsi le produit scalaire euclidien est un produit scalaire réel.

Au lieu de noter f *(X; Y) on note souvent :*

$$f(X ; Y) = X \cdot Y$$

Et les axiomes s'écrivent :

$\boxed{S_1}$ $(\forall X_1)(\forall X_2)(\forall Y)$ $(X_1 + X_2)\cdot Y = X_1 \cdot Y + X_2 \cdot Y.$

$\boxed{S_2}$ $(\forall \lambda)(\forall X)$ $(\lambda X)\cdot Y = \lambda(X \cdot Y).$

$\boxed{S_3}$ $(\forall X)(\forall Y)$ $X \cdot Y = Y \cdot X.$

$\boxed{S_4}$ $(\forall X)$ $X \cdot X > 0$ si $X \in E^*.$

$\boxed{S_1}$ est une distributivité à droite.

$\boxed{S_2}$ est une associativité mixte.

$\boxed{S_3}$ est une commutativité.

Pour le produit scalaire réel, la distributivité à droite $\boxed{S_1}$ et la commutativité $\boxed{S_3}$ impliquent la distributivité à gauche.

De même :

$$X \cdot (\lambda Y) = \lambda \cdot (X \cdot Y)$$

De plus, si dans $\boxed{S_2}$ on fait $\lambda = 0$, on a :

$$0 \cdot Y = 0$$

On note souvent :

$$X \cdot X = X^2$$

et alors :

$$X^2 = 0 \Leftrightarrow X = 0.$$

Remarque 1.

Souvent, par abus de langage, le nombre réel $X \cdot Y = f(X; Y)$ est appelé le produit scalaire des vecteurs X et Y.

Remarque 2.

Lorsque l'espace vectoriel E est construit sur le corps C des complexes on peut définir un *produit scalaire complexe* à l'aide des axiomes $\boxed{S_1}$ $\boxed{S_2}$ $\boxed{S_4}$. L'axiome $\boxed{S_3}$ est remplacé par un axiome différent $\boxed{S'_3}$.

$\boxed{S'_3}$ $(\forall X)(\forall Y)$ $X \cdot Y = \overline{Y \cdot X}$

$\overline{Y \cdot X}$ désigne le complexe conjugué de $Y \cdot X$.

508. Normes.

De même que la notion de produit scalaire a été axiomatisée, la notion de norme peut aussi être axiomatisée.

Soient *un espace vectoriel sur le corps R ou le corps C*, et une application N de E dans R_+ :

N : $X \in E \longrightarrow N(X) \in R_+.$

L'application N est une norme si elle vérifie les axiomes suivants :

$\boxed{N_1}$ $(\forall X)$ $N(X) = 0 \Leftrightarrow X = 0.$

$\boxed{N_2}$ $(\forall \lambda)(\forall X)$ $N(\lambda X) = |\lambda| \cdot N(X).$

$\boxed{N_3}$ $(\forall X)(\forall Y)$ $N(X + Y) \leqslant N(X) + N(Y).$

On note aussi :

$$N(X) = \|X\|.$$

Par abus de langage le nombre positif N (X) = ‖ X ‖ est appelé la norme du vecteur X.

Ici encore il est possible de déduire de ces trois axiomes des propriétés qui, dès lors, sont vraies pour toutes les normes.

Ainsi :

1° On a :

$$\|-X\| = \|(-1)\cdot X\| = |-1|\cdot\|X\| = \|X\|.$$

D'où :

$$\|-X\| = \|X\|. \qquad (508;1)$$

Et :

Deux vecteurs opposés ont la même norme.

2° On a :

$$\|X - Y\| = \|X + (-Y)\| \leqslant \|X\| + \|-Y\| = \|X\| + \|Y\|.$$

D'où :

$$\|X - Y\| \leqslant \|X\| + \|Y\|. \qquad (508;2)$$

3° Si $\|X\| \geqslant \|Y\|$, on écrit :

$$\|X\| = \|X + Y - Y\| \leqslant \|X + Y\| + \|Y\|.$$

D'où :

$$\|X\| - \|Y\| \leqslant \|X + Y\|. \qquad (508;3)$$

Si $\|X\| \leqslant \|Y\|$, on écrit :

$$\|Y\| = \|X + Y - X\| \leqslant \|X + Y\| + \|X\|.$$

D'où :

$$\|Y\| - \|X\| \leqslant \|X + Y\|. \qquad (508;4)$$

Les résultats (508; 3) et (508; 4) se groupent :

$$\big|\|X\| - \|Y\|\big| \leqslant \|X + Y\|. \qquad (508;5)$$

Dans tous les cas, on a donc :

$$\big|\|X\| - \|Y\|\big| \leqslant \|X + Y\| \leqslant \|X\| + \|Y\|. \qquad (508;6)$$

4° En remplaçant dans (508; 6), Y par — Y on a :

$$\big|\|X\| - \|Y\|\big| \leqslant \|X - Y\| \leqslant \|X\| + \|Y\|. \qquad (508;7)$$

◇ *Exemple de norme.*

Si l'espace vectoriel E sur R est muni d'un produit scalaire réel

$$N(X) = \sqrt{X \cdot X} = \sqrt{X^2}$$

est une norme.

509. Orthogonalité.

La notion d'orthogonalité peut s'axiomatiser, en se débarrassant de son intuition physique.

Soit un espace vectoriel E sur R muni d'un produit scalaire réel.

Deux éléments X et Y de E sont dits orthogonaux si leur produit scalaire est nul :

$$(X \perp Y) \iff (X \cdot Y = 0).$$

On a défini et étudié ainsi l'orthogonalité des vecteurs de R^2 ou de R^3. Mais la définition est générale; c'est ainsi que, dans des classes ultérieures, on parlera de polynômes orthogonaux.

510. Distances.

1° Toutes les notions précédentes, qui ont été axiomatisées, avaient déjà été rencontrées une ou plusieurs fois dans cette première partie du cours. On se propose d'étudier maintenant l'axiomatique d'une notion non encore rencontrée : la notion de distance.

Soit un ensemble E d'éléments appelés points : $E = \{A; B; C; \ldots\}$.

On envisage une application d de E × E dans R_+ :

$$d: \qquad (A;B) \in E \times E \longrightarrow d(A;B) \in R_+$$

L'application d est une distance si elle vérifie les axiomes suivants :

$\boxed{M_1}$ $(\forall A)(\forall B)$ $\quad d(A;B) = 0 \iff A = B.$

$\boxed{M_2}$ $(\forall A)(\forall B)$ $\quad d(A;B) = d(B;A).$

$\boxed{M_3}$ $(\forall A)(\forall B)(\forall C)$ $\quad d(A;B) \leqslant d(A;C) + d(C;B).$

$\boxed{M_1}$ est l'axiome de séparation ;

$\boxed{M_2}$ est l'axiome de symétrie ;

$\boxed{M_3}$ est l'axiome de l'inégalité triangulaire.

Si d est une distance, l'ensemble $\{E; d\}$ est un *espace ponctuel métrique*.

Par abus de langage, on dit que le nombre positif* d *(A; B) est la distance du point A au point B.

Il est possible de déduire de ces trois axiomes des propriétés qui, dès lors, sont vraies pour toutes les distances.

2° Si :

$$d\,(A; C) \leqslant d\,(B; C)$$

on a :

$$d\,(A; C) \leqslant d\,(A; B) + d\,(B; C)$$

D'où :

$$d\,(A; C) - d\,(B; C) \leqslant d\,(A; B) \qquad (510; 1)$$

Si :

$$d\,(A; C) \leqslant d\,(B; C)$$

on a :

$$d\,(B; C) \leqslant d\,(B; A) + d\,(A; C)$$

D'où

$$d\,(B; C) - d\,(A; C) \leqslant d\,(A; B) \qquad (510; 2)$$

Les résultats (510; 1) et (510; 2) se groupent :

$$|d\,(A; C) - d\,(B; C)| \leqslant d\,(A; B) \qquad (510; 3)$$

Dans tous les cas, on a donc :

$$\mathbf{|d(A; C) - d(B; C)| \leqslant d(A; B) \leqslant d(A; C) + d(B; C).} \qquad (510; 4)$$

Ainsi si dans la suite du cours, une application d vérifie les trois axiomes $\boxed{M_1}$ $\boxed{M_2}$ $\boxed{M_3}$ elle prendra le nom de distance; et, sans aucune démonstration, on pourra affirmer qu'elle possède la propriété (510; 4).

511. Étude d'un isomorphisme.

Les exposés des chapitres sur l'espace vectoriel K^3 et sur l'espace vectoriel $\mathcal{M}_1^3$ (cf. n°s 351 à 371) sont presque identiques; il est intéressant de rechercher la nature de cette analogie.

On envisage l'application φ suivante :

$$\varphi : \qquad A = (x; y; z) \in K^3 \longrightarrow \varphi(A) = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathcal{M}_1^3.$$

Cette application φ *est une bijection de* K^3 *sur* $\mathcal{M}_1^3$; en effet un vecteur quelconque $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ de $\mathcal{M}_1^3$ est l'image d'un et d'un unique vecteur $(x; y; z)$ de K^3.

Soient maintenant les deux vecteurs :

$$A = (x; y; z)$$
$$B = (x'; y'; z')$$

et leur somme

$$A + B = (x + x'; y + y'; z + z').$$

D'autre part :

$$\varphi(A) = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \qquad \text{et} \qquad \varphi(B) = \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$$

D'où :

$$\varphi(A) + \varphi(B) = \begin{pmatrix} x \\ y \\ z \end{pmatrix} + \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$$
$$= \begin{pmatrix} x + x' \\ y + y' \\ z + z' \end{pmatrix}$$

Or :

$$\varphi(A + B) = \begin{pmatrix} x + x' \\ y + y' \\ z + z' \end{pmatrix}$$

Par suite :

$$\varphi(A + B) = \varphi(A) + \varphi(B). \qquad (511; 1)$$

La bijection φ ***est appelée un isomorphisme pour les additions dans*** K^3 ***et*** $\mathcal{M}_1^3$,

ou encore :

L'addition dans $\mathcal{M}_1^3$ ***et l'addition dans*** K^3 ***sont isomorphes.***

Soient encore :

$$\alpha \in K, \quad A = (x; y; z) \in K^3$$

et

$$\alpha \cdot A = (\alpha x; \alpha y; \alpha z).$$

On a :

$$\varphi(\alpha \cdot A) = \begin{pmatrix} \alpha \cdot x \\ \alpha \cdot y \\ \alpha \cdot z \end{pmatrix}$$

D'autre part :

$$\alpha \cdot \varphi(A) = \alpha \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \alpha \cdot x \\ \alpha \cdot y \\ \alpha \cdot z \end{pmatrix}$$

Par suite :

$$\varphi(\alpha \cdot A) = \alpha \cdot \varphi(A). \qquad (511 ; 2)$$

La bijection est un isomorphisme pour les lois externes dans K^3 ***et*** $\mathcal{M}_1^3$.

En résumé :

La bijection φ ***est un isomorphisme de l'espace vectoriel*** K^3 ***sur l'espace vectoriel*** $\mathcal{M}_1^3$.

K^3 et $\mathcal{M}_1^3$ sont des espaces isomorphes.

512. Etude d'un homomorphisme.

On considère maintenant l'espace vectoriel K^3 et l'espace vectoriel K^2 On envisage l'application φ définie par :

$$\varphi : \qquad (x ; y ; z) \in K^3 \longrightarrow \varphi(x ; y ; z) = (x ; y) \in K^2.$$

L'application φ n'est pas une bijection car :

$$(\forall z) \quad \varphi\,(a; b; z) = (a; b)$$

Soient les vecteurs de K^3 :

$$A = (x; y; z)$$
$$B = (x'; y'; z')$$

et

$$A + B = (x + x'; y + y'; z + z')$$

D'autre part :

$$\varphi\,(A) = (x; y)$$
$$\varphi\,(B) = (x'; y')$$
$$\varphi\,(A + B) = (x + x'; y + y')$$

Or :

$$\varphi\,(A) + \varphi\,(B) = (x; y) + (x'; y') = (x + x'; y + y')$$

Par suite :

$$\varphi\,(A + B) = \varphi\,(A) + \varphi\,(B) \qquad (512; 1)$$

L'application φ ***est un homomorphisme de l'addition de*** K^3 ***sur l'addition dans*** K^2.

On a encore : $\varphi(\alpha \cdot A) = \varphi(\alpha x; \alpha y; \alpha z)$
$= (\alpha x; \alpha y)$

et

$$\alpha \cdot \varphi(A) = \alpha \cdot (x; y) = (\alpha x; \alpha y)$$

Par suite :

$$\varphi(\alpha \cdot A) = \alpha \cdot \varphi(A)$$

L'application φ est un homomorphisme de la loi externe dans K^3 sur la loi externe dans K^2.

513. Homomorphismes et isomorphismes.

On peut généraliser les idées précédentes.

1° Soient un ensemble E muni d'une loi interne notée $*$, et un ensemble F muni d'une loi interne notée T.

On considère l'application φ de E dans F :

φ : $x \in E \longrightarrow \varphi(x) \in F$.

Si l'application φ possède la propriété suivante :

$$\varphi(\mathbf{x} * \mathbf{y}) = \varphi(\mathbf{x}) \top \varphi(\mathbf{y}).$$

on dit que φ est un homomorphisme de la loi $*$ de E et de la loi $\top$ de F.

Ou encore :

φ est un homomorphisme si l'image du composé de deux éléments de E est le composé dans F des images des deux éléments de F.

2° ***Si φ est une bijection et un homomorphisme, φ est un isomorphisme.***

◇ *Exemple.*

Soit $E = N$ et $F = \{2^n / n \in N\}$. On envisage :

φ : $n \in N \longrightarrow \varphi(n) = 2^n$.

On a :

$$\varphi(n) = 2^n$$
$$\varphi(m) = 2^m$$
$$\varphi(n + m) = 2^{n+m}$$

et

$$\varphi(n) \cdot \varphi(m) = 2^n \cdot 2^m = 2^{n+m}$$

Donc :

$$\varphi(n + m) = \varphi(n) \cdot \varphi(m)$$

Par suite :

φ est isomorphisme de $\{ N; + \}$ sur $\{ F; \times \}$.

514. Rôle des homomorphismes.

Soit un homomorphisme φ de l'ensemble { E; ✳ } sur l'ensemble { F; T }.

On démontre que si { E; ✳ } est muni d'une structure algébrique, alors φ (E) ⊂ F est muni de la même structure algébrique.

Par suite, si { E; ✳ } est, par exemple, un anneau, alors φ(E) est un anneau.

L'homomorphisme apparaît donc comme un procédé de démonstration efficace, qui réalise une économie de pensée très importante.

515. Conclusion.

Dans ce chapitre, à partir d'exemples étudiés auparavant on a montré la nécessité d'axiomatiser les notions de base des mathématiques : groupe, anneau, espace vectoriel, norme, etc. Mais aussi, sans exemples précédents, on a axiomatisé la notion de distance. Le but de ces axiomatisations est de réaliser des synthèses fructueuses accompagnées d'une appréciable économie de pensée.

Ainsi sont mises en évidence les raisons de l'axiomatique.

Le lecteur est alors à l'orée de la Mathématique de notre temps. Puisse cet exposé l'inciter à entreprendre l'exploration de cette mathématique moderne passionnante et combien captivante !

CHAPITRE XXXVII

PROBLÈMES

516. Problème 1.

1° Soit un groupe $G = \{ G; \ast \}$. Quand peut-on dire qu'une partie H de G est un sous-groupe de G?

2° Dans l'ensemble $G = Q^* \times Q$ des couples de rationnels on introduit une loi notée $\ast$ et définie par

$$(a; b) \ast (a'; b') = (aa'; ba' + b').$$

$\{ G; \ast \}$ est-il un groupe?

On considère l'ensemble H des éléments de G qui sont de la forme (1; b); $\{ H; \ast \}$ est-il un sous-groupe de $\{ G; \ast \}$.

3° Soit $E = \{ a; b; c \}$ un ensemble de trois éléments distincts. Quelles sont les permutations de E? Soit G l'ensemble de ces permutations.

On introduit la loi $_0$ de composition des permutations. Quelle est la structure de G? Y a-t-il des sous-groupes.

4° On considère un triangle équilatéral ABC. Quelles sont les isométries planes qui conservent ce triangle équilatéral. Soit Γ l'ensemble de ces isométries.

Montrer que Γ est isomorphe de G dans 2°. Quelle est la structure de Γ?

1° Il peut arriver que la partie H de G munie de la loi $\ast$ ait une structure de groupe. On dit alors que H est un sous-groupe de G.

Autrement dit, la restriction de la loi $\ast$ à H doit faire de H un groupe.

Il faut donc vérifier que

$$(a \in H \text{ et } b \in H) \Rightarrow (a \ast b \in H)$$

et que les axiomes [A] [N] [S] sont vérifiés dans H.

L'axiome d'associativité est vérifié dans G, donc dans H.

Le neutre e existe; il suffit donc de vérifier que e appartient à H.

Tout élément a possède un symétrique a'; il suffit de vérifier que si a appartient à H son symétrique a' appartient à H.

2° La loi $\divideontimes$ d'après sa définition est une loi interne car :

$$(a \in Q^*,\ b \in Q,\ a' \in Q^*,\ b' \in Q) \Rightarrow (aa' \in Q^* \text{ et } ba' + b' \in Q)$$

Il faut vérifier les trois axiomes d'un groupe.

Associativité.

Soient

$$\alpha = (a; b) \qquad \alpha' = (a'; b') \qquad \alpha'' = (a''; b'')$$

On a :

$$\begin{aligned}(\alpha \divideontimes \alpha') \divideontimes \alpha'' &= (aa'; ba' + b') \divideontimes (a''; b'') \\ &= [aa'a''; (ba' + b')\, a'' + b''] \\ &= (aa'a''; ba'a'' + b'a'' + b'')\end{aligned}$$

et

$$\begin{aligned}\alpha \divideontimes (\alpha' \divideontimes \alpha'') &= (a; b) \divideontimes (a'a''; b'a'' + b'') \\ &= [(aa'a''; ba'a'' + (b'a'' + b'')]\end{aligned}$$

Les deux résultats sont identiques; donc :

[A] $\qquad (\forall \alpha)(\forall \alpha')(\forall \alpha'') \quad (\alpha \divideontimes \alpha') \divideontimes \alpha'' = \alpha \divideontimes (\alpha' \divideontimes \alpha'')$

Existence d'un neutre.

L'élément $e = (1; 0)$ est neutre; en effet :

$$\begin{aligned}\alpha \divideontimes e &= (a; b) \divideontimes (1; 0) \\ &= (a; b) \\ &= \alpha\end{aligned}$$

et

$$\begin{aligned}e \divideontimes \alpha &= (1; 0) \divideontimes (a; b) \\ &= (a; b) \\ &= \alpha.\end{aligned}$$

Donc :

[N] $\qquad (\exists e)(\forall \alpha) \quad \alpha \divideontimes e = e \divideontimes \alpha = \alpha.$

Existence d'un symétrique.

Soit $\alpha = (a; b)$. On se propose de déterminer α' tel que $\alpha\alpha' = \alpha'\alpha = e$. On pose :

$$\alpha' = (x; y).$$

D'où :

$$\alpha \cdot \alpha' = (a; b) \ast (x; y)$$
$$= (ax; bx + y)$$

On doit donc avoir :

$$\begin{cases} ax = 1 \\ bx + y = 0 \end{cases}$$

D'où :

$$x = \frac{1}{a}$$

ce qui suppose $a \neq 0$.

D'où :

$$y = -\frac{b}{a}.$$

Le symétrique α' ne peut être que $\left(\frac{1}{a}; -\frac{b}{a}\right)$. Il faut encore vérifier que $\alpha' \cdot \alpha = e$.

On a :

$$\alpha' \cdot \alpha = \left(\frac{1}{a}; -\frac{b}{a}\right) \ast (a; b)$$
$$= \left(\frac{1}{a} \cdot a; -\frac{b}{a} \cdot a + b\right)$$
$$= (1; 0)$$
$$= e.$$

Donc :

$$\alpha' = \left(\frac{1}{a}; -\frac{b}{a}\right) \text{ est le symétrique de } \alpha = (a; b).$$

N $\quad (\forall\alpha)(\exists\alpha') \quad \alpha \ast \alpha' = \alpha' \ast \alpha = e.$

Finalement :

G est un groupe (non commutatif).

On considère maintenant l'ensemble H des éléments de la forme $(1; b)$; c'est bien une partie de G.

La loi $\ast$ est une loi interne pour H; en effet :

$$\alpha \ast \alpha' = (1; b) \ast (1; b')$$
$$= (1; b + b').$$

Cette loi $*$ munit H d'une structure de groupe. En effet :
l'associativité dans G implique l'associativité dans H;
le neutre $e = (1; 0)$ appartient à H;
l'élément $\alpha = (1; b)$ a pour symétrique $\alpha' = (1; -b)$ et α' appartient à H.

Finalement :

H est un sous-groupe de G.

3° Soit l'ensemble $E = \{a; b; c\}$. Il y a $3! = 6$ permutations de E. Ce sont :

$$e : \begin{cases} a \longrightarrow a \\ b \longrightarrow b \\ c \longrightarrow c \end{cases} \qquad \lambda : \begin{cases} a \longrightarrow b \\ b \longrightarrow c \\ c \longrightarrow a \end{cases} \qquad \mu : \begin{cases} a \longrightarrow c \\ b \longrightarrow a \\ c \longrightarrow b \end{cases}$$

$$\alpha : \begin{cases} a \longrightarrow a \\ b \longrightarrow c \\ c \longrightarrow b \end{cases} \qquad \beta : \begin{cases} a \longrightarrow c \\ b \longrightarrow b \\ c \longrightarrow a \end{cases} \qquad \gamma : \begin{cases} a \longrightarrow b \\ b \longrightarrow a \\ c \longrightarrow c \end{cases}$$

Soit $G = \{e; \lambda; \mu; \alpha; \beta; \gamma\}$. Le produit de deux permutations est une permutation; donc la loi de composition notée $_o$ est une loi interne dans G.

Cette loi est associative; car la loi de composition des applications est associative.

e est neutre pour la loi $_o$.

Chaque élément est inversible.

D'ailleurs ici il est intéressant de construire la table de composition. Par exemple :

$$\lambda {}_o \beta = \alpha$$

car :

$$\begin{array}{ccccc} & \beta & & \lambda & \\ a & \longrightarrow & c & \longrightarrow & a \\ b & \longrightarrow & b & \longrightarrow & c \\ c & \longrightarrow & a & \longrightarrow & b \end{array}$$

Donc :

$$\lambda_o \beta : \begin{cases} a \longrightarrow a \\ b \longrightarrow c \\ c \longrightarrow b \end{cases}$$

ou

$$\lambda_o \beta = \alpha.$$

On obtient facilement :

	e	λ	μ	α	β	γ
e	e	λ	μ	α	β	γ
λ	λ	μ	e	γ	α	β
μ	μ	e	λ	β	γ	α
α	α	β	γ	e	λ	μ
β	β	γ	α	μ	e	λ
γ	γ	α	β	λ	μ	e

Dans la première colonne on a placé les éléments à gauche du signe $_o$; dans la première ligne les éléments à droite du signe $_o$ (cf. n° 87; 3°).

Le tableau montre que e est neutre; que e, λ, μ, α, β, γ ont respectivement pour symétrique e, μ, λ, α, β, γ, que la loi n'est pas commutative.

Finalement :

G est un groupe non commutatif.

4° Les isométries du triangle équilatéral de centre O sont :

la transformation identique : ε;
la rotation de centre O et d'angle 120° : r;
la rotation de centre O et d'angle — 120° : s;
la symétrie pour la hauteur passant par A : a;
la symétrie pour la hauteur passant par B : b;
la symétrie pour la hauteur passant par C : c.

Soit : $\Gamma = \{\varepsilon; r; s; a; b; c\}$

On considère la bijection :

$$\begin{aligned} \varphi : e &\longrightarrow \varphi(e) = \varepsilon \\ \lambda &\longrightarrow \varphi(\lambda) = r \\ \mu &\longrightarrow \varphi(\mu) = s \\ \alpha &\longrightarrow \varphi(\alpha) = a \\ \beta &\longrightarrow \varphi(\beta) = b \\ \gamma &\longrightarrow \varphi(\gamma) = c \end{aligned}$$

On a par exemple :

$$\lambda \circ \beta = \alpha$$

et

$$r \circ b = a$$

D'où

$$\varphi(\lambda \circ \beta) = \varphi(\alpha)$$

ou

$$\varphi(\lambda \circ \beta) = \varphi(\lambda) \circ \varphi(\beta)$$

et φ ***est un isomorphisme de G sur F.***

Donc :

Γ ***est un groupe non commutatif.***

517. Problème 2.

1° On considère l'anneau Z des entiers rationnels. Soit un nombre naturel p. *(*p $\in$ *N).*
Montrer que l'ensemble des multiples de p *est un sous-groupe additif commutatif de Z. On note H =* p*Z.*

Montrer que :

$$[(\forall z)\ (z \in Z),\ (\forall x)\ (x \in H)] \Rightarrow (zx \in H) \qquad (1)$$

On dit alors que H = p*Z est un idéal de Z et que cet idéal est engendré par* p *ou que H est un idéal principal.*

2° On appelle idéal de Z toute partie H de Z telle que H soit un sous-groupe additif de Z et possède la propriété (1).
Démontrer que tous les idéaux de Z sont principaux.

3° Soient deux entiers rationnels a *et* b *(*a $\in$ *Z;* b $\in$ *Z). On considère l'ensemble*

$$H = \{x \cdot a + y \cdot b \ / \ x \in Z \text{ et } y \in Z\}$$

Montrer que H est un idéal de Z.

4° Montrer que H est engendré par $\delta = a \wedge b$.

5° Démontrer que :

$$(\exists u)(\exists v) : \quad au + bv = \delta.$$

6° Démontrer l'équivalence :

$$[a \wedge b = 1] \quad \Leftrightarrow \quad [(\exists u)(\exists v)\ au + bv = 1].$$

7° Soit K l'ensemble des multiples communs à a *et* b. *Montrer que K est un idéal de Z.*

8° Montrer que K est engendré par $\mu = a \vee b$.

1° Soient deux éléments de $H = pZ$

$$\alpha = pa \in H \qquad \beta = pb \in H.$$

D'où :

$$\alpha + \beta = p\,(a + b)$$

et

$$\alpha + \beta \in H$$

L'addition est une loi interne dans H.

Cette addition est associative; le neutre $0 = p \cdot 0$ appartient à H; le symétrique de $\alpha = pa$ est $\alpha' = -pa = p \cdot (-a)$ et α' appartient à H.

Donc :

H est un sous-groupe additif commutatif de Z.

De plus soit $x = pa$ un élément de H. Pour tout nombre rationnel z, on a :

$$zx = z \cdot pa$$
$$= p \cdot (za)$$

et

$$zx \in H.$$

H est un idéal principal de Z.

2° Soit H un idéal quelconque de Z; soit $p \in N^*$ le plus petit nombre naturel appartenant à H.

Si a est un élément quelconque de H, en divisant a par p, on a :

$$a = p \cdot b + r \qquad r < p \qquad \text{et} \qquad r > 0$$

En supposant $r \neq 0$, on a :

$$pb \in H$$

et

$$a - pb \in H$$

Donc :

$$r \in H.$$

Or cela n'est possible, d'après la définition de p, que si $r = 0$.

Autrement dit :

Si p est le plus petit nombre naturel non nul appartenant à un idéal H de Z, quel que soit le nombre a de H, il existe un nombre b tel que $a = p \cdot b$. H est engendré par p.

Et :

Tous les idéaux de Z sont des idéaux principaux.

3° Soient les entiers rationnels a et b. On considère l'ensemble

$$H = \{ x \cdot a + y \cdot b \;/\; x \in Z \quad \text{et} \quad y \in Z \}$$

et on se propose de démontrer que H est un idéal de Z.

Soient :

$$m_1 = x_1 \cdot a + y_1 \cdot b \qquad \text{et} \qquad m_2 = x_2 \cdot a + y_2 \cdot b$$

D'où :

$$m_1 + m_2 = (x_1 + x_2) \cdot a + (y_1 + y_2) \cdot b$$

et

$$m_1 + m_2 \in \text{H}.$$

L'addition est une loi interne dans H.

Cette addition est évidemment associative; le neutre 0 appartient à H ($x = 0; y = 0$); l'opposé de m_1 appartient à H ($x = -x_1; y = -y_1$).

Donc :

H est un sous-groupe additif de Z.

De plus :

$$(\forall z)\ (z \in Z) : \quad z\,(x \cdot a + y \cdot b) = (zx) \cdot a + (zy) \cdot b \ \in \text{H}$$

En définitive :

H est un idéal de Z.

4° Comme dans Z tous les idéaux sont principaux, H est un idéal principal; il est engendré par un nombre naturel non nul δ, qui est le plus petit possible dans H.

Donc :

Tout diviseur de a et b divise tous les nombres $x \cdot a + b \cdot y$, donc divise tous les multiples de δ; en particulier divise δ.

Tous les diviseurs communs à a et b *sont diviseurs de* δ.

Le plus grand des diviseurs communs à a et b est donc le plus grand diviseur de δ, c'est-à-dire δ :

***Le P.G.C.D. de* a et b *est donc* δ.**

5° Soient a, b, et leur P.G.C.D. : $\delta = a \wedge b$.

D'après ce qui précède, puisque $\delta \in \text{H}$, il existe deux nombres entiers rationnels tels que

$$a \cdot u + b \cdot v = \delta$$

Ce résultat est connu sous le nom de *théorème de Bezout*.

6° *Les deux assertions :*

α) a et b *sont premiers entre eux;*
β) $(\exists u)\ (\exists v) : a \cdot u + b \cdot v = 1$

sont équivalentes.

En effet :

$\alpha) \Rightarrow \beta)$ Puisque $a \wedge b = 1$, d'après le théorème de Bezout, il existe deux nombres u et v tels que $au + bv = 1$.

$\beta) \Rightarrow \alpha)$ Par hypothèse il existe deux nombres u et v tels que $au + bv = 1$. Par suite l'idéal $H = \{ ax + by / x \in Z \text{ et } y \in Z \}$ contient $au + bv = 1$; donc H est engendré par 1; autrement dit $\delta = a \wedge b = 1$.

Cette condition nécessaire et suffisante pour que deux nombres soient premiers entre eux est connue sous le nom de *condition de Bezout*.

7° On considère maintenant l'ensemble K des multiples communs à a et b. K contient au moins ab, donc contient des éléments autres que 0. On se propose de démontrer que K est un idéal de Z.

Soient deux éléments M_1 et M_2 de K; on a :

$$M_1 = ma = nb$$
$$M_2 = m'a = n'b$$

D'où :

$$M_1 + M_2 = (m + m')\,a = (n + n')\,b$$

et

$$M_1 + M_2 \in K.$$

L'addition est une loi interne dans K.

Cette addition est évidemment associative; le neutre 0 appartient à K ($m = 0$ et $n = 0$); l'opposé de M_1 appartient à K.

Donc :

K est un sous-groupe additif de Z.

De plus :

$$(\forall z)\ (z \in Z) : \quad z \cdot M = z \cdot (ma) = z \cdot (nb) = (z \cdot m)\,a = (z \cdot n)\,b \in K$$

En définitive :

K est un idéal de Z.

8° Comme dans Z tous les idéaux principaux, K est un idéal principal; il est engendré par un nombre naturel non nul μ, qui est le plus petit possible dans K.

Donc :

Tout multiple commun de a *et* b *est multiple de* μ.

Le plus petit des diviseurs positifs communs à a et b est donc le plus petit multiple de μ, c'est-à-dire μ.

Le P.P.C.M. de a et b est donc μ.

518. Problème 3.

On considère l'ensemble E des nombres de la forme a + b $\sqrt{3}$, a et b étant des nombres rationnels. E est muni de l'addition et de la multiplication ordinaire.

1° Montrer que E est un corps commutatif.

2° Soient les ensembles Q et E', E' étant l'ensemble des nombres de la forme b $\sqrt{3}$. Quelles sont les structures de ces sous-ensembles de E?

3° Dans F = Q^2, on introduit les deux lois :

$$(a; b) + (a'; b') = (a + a'; b + b')$$
$$(a; b) \cdot (a'; b') = (aa' + 3bb'; ab' + ba').$$

Quelle est la structure de F?

4° On considère l'application φ définie par :

$$\varphi : \quad (a + b\sqrt{3}) \in E \longrightarrow \varphi(a + b\sqrt{3}) = (a; b) \in F.$$

Montrer que φ est un isomorphisme.

1° Il faut montrer que l'addition et la multiplication sont des lois internes; puis vérifier les axiomes d'un corps commutatif.

Addition.

Soient : $\alpha = a + b\sqrt{3}$ et $\alpha' = a' + b'\sqrt{3}$.

On a :

$$\alpha + \alpha' = (a + a') + (b + b')\sqrt{3}$$

L'addition est une loi interne.

Comme E est une partie stable de R, l'associativité et la commutativité sont évidentes. Le neutre est 0; il correspond à $a = 0$ et $b = 0$; il appartient à E. Le symétrique de $\alpha = a + b\sqrt{3}$ est $-\alpha = (-a) + (-b)\sqrt{3}$; il appartient à E.

Donc :

E est un sous-groupe additif commutatif de R.

Multiplication.

Soient : $\alpha = a + b\sqrt{3}$ et $\alpha' = a' + b'\sqrt{3}$.

On a :

$$\alpha\alpha' = (a + b\sqrt{3})(a' + b'\sqrt{3})$$
$$= (aa' + 3bb') + (ab' + ba')\sqrt{3}.$$

Or : $aa' + 3bb'$ et $ab' + ba'$ sont des rationnels. Et :
La multiplication est une loi interne.

Comme E est une partie stable de R, l'associativité et la commutativité sont évidentes.

Le neutre est 1; il correspond à $a = 1$ et $b = 0$; il appartient à E.

On pose maintenant $E^* = E - \{0\}$. $\alpha = a + b\sqrt{3}$ étant un élément de E*, on se propose de chercher son inverse; si $\alpha' = x + y\sqrt{3}$ est un inverse de α, on doit avoir :

$$(a + b\sqrt{3}) \cdot (x + y\sqrt{3}) = 1$$

d'où :

$$\begin{aligned} x + y\sqrt{3} &= \frac{1}{a + b\sqrt{3}} \\ &= \frac{a - b\sqrt{3}}{a^2 - 3b^2} \\ &= \frac{a}{a^2 - 3b^2} + \frac{-b}{a^2 - 3b^2}\sqrt{3}. \end{aligned}$$

Comme $a^2 - 3b^2$ ne s'annule que dans Q que pour $a = b = 0$, on a bien

$$x = \frac{a}{a^2 - 3b^2} \qquad \text{et} \qquad y = -\frac{b}{a^2 - 3b^2}.$$

L'inverse d'un élément de E* appartient à E*.

Donc :

E est un sous-groupe multiplicatif commutatif de R.*

Distributivité.

E étant une partie stable pour l'addition et la multiplication dans R, la distributivité est évidente.

Par suite :

E est un corps commutatif.

2° Q est l'ensemble des éléments de E de la forme $a + 0 \cdot \sqrt{3}$; c'est donc un sous-corps commutatif de E.

Quand à E' c'est un sous-groupe additif de E.

Comme la multiplication de $\alpha = b\sqrt{3}$ et de $\alpha' = b'\sqrt{3}$ donne

$$\alpha\alpha' = 3bb'$$

on voit que la multiplication n'est pas une loi interne dans E. Par suite E n'est ni un anneau, ni un corps.

3° On va étudier successivement l'addition et la multiplication dans F.

Addition. L'addition est manifestement une loi interne.

Soient $\alpha = (a; b) \qquad \alpha' = (a'; b') \qquad \alpha'' = (a''; b'')$

On a :

$$(\alpha + \alpha') + \alpha'' = (a + a' + a''; b + b' + b'')$$

et

$$\alpha + (\alpha' + \alpha'') = (a + a' + a''; b + b' + b'').$$

Donc :

A $\quad (\forall\alpha)(\forall\alpha')(\forall\alpha'') : \quad (\alpha + \alpha') + \alpha'' = \alpha + (\alpha' + \alpha'').$

L'élément $e = (0; 0)$ est neutre pour l'addition :

N $\quad (\forall\alpha) \qquad \alpha + e = e + \alpha = \alpha.$

L'opposé de $\alpha = (a; b)$ est $a' = (-a; -b)$:

S $\quad (\forall\alpha)(\exists\alpha') \qquad \alpha + \alpha' = \alpha' + \alpha = e.$

Enfin l'addition est visiblement commutative :

C $\quad (\forall\alpha)(\forall\alpha') \qquad \alpha + \alpha' = \alpha' + \alpha.$

Multiplication.

La multiplication est visiblement une loi interne.

On a :

$$\begin{aligned}(\alpha\alpha')\,\alpha'' &= (aa' + 3bb'; ab' + ba') \cdot (a''; b'') \\ &= (aa'a'' + 3bb'a'' + 3ab'b'' + 3ba'b''; aa'b'' + 3bb'b'' + \\ &\qquad ab'a'' + ba'a'')\end{aligned}$$

et

$$\begin{aligned}\alpha\,(\alpha'\alpha'') &= (a; b) \cdot (a'a'' + 3b'b''; a'b'' + b'a'') \\ &= (aa'a'' + 3ab'b'' + 3ba'b'' + 3bb'a''; aa'b'' + ab'a'' + \\ &\qquad ba'a'' + 3bb'b'').\end{aligned}$$

Donc :

A $\quad (\forall\alpha)(\forall\alpha')(\forall\alpha'') \qquad (\alpha \cdot \alpha')\,\alpha'' = \alpha \cdot (\alpha'\alpha'').$

La commutativité est évidente :

C $\quad (\forall\alpha)(\forall\alpha') \qquad \alpha \cdot \alpha' = \alpha' \cdot \alpha.$

Le neutre pour la multiplication est $\varepsilon = (1; 0)$; en effet :

$$\begin{aligned}\alpha \cdot \varepsilon &= (a; b) \cdot (1; 0) \\ &= (a; b) \\ &= \alpha.\end{aligned}$$

Donc :

N $\quad (\forall\alpha) \qquad \alpha \cdot \varepsilon = \varepsilon \cdot \alpha = \alpha.$

On pose maintenant $F^* = F - \{e\}$. $\alpha = (a; b)$ étant un élément de F^*, on se propose de chercher son inverse; si $\alpha' = (x; y)$ est un inverse de α, on doit avoir

$$(a; b)\,(x; y) = \varepsilon$$

ou

$$(ax + 3by;\ ay + bx) = (1; 0).$$

D'où le système :

$$\begin{cases} ax + 3by = 1 \\ bx + ay = 0 \end{cases}$$

Puisque α appartient à F^* et que $a^2 - 3b^2$ n'est nul dans Q que pour $a = b = 0$, le système précédent admet une solution unique :

$$\begin{cases} x = \dfrac{a}{a^2 - 3b^2} \\ y = \dfrac{-b}{a^2 - 3b^2} \end{cases}$$

Donc :

$\boxed{S}$ $\qquad (\forall\alpha)(\alpha \in F^*), (\exists\alpha') \qquad \alpha \cdot \alpha' = \alpha' \cdot \alpha = \varepsilon.$

Distributivité.

Soient : $\quad \alpha = (a; b) \qquad \alpha' = (a'; b') \qquad \mu = (x; y).$

On a :

$$\begin{aligned} \mu\,(\alpha + \alpha') &= (x; y)\,(a + a'; b + b') \\ &= (ax + a'x + 3by + 3b'y;\ bx + b'x + ay + a'y) \end{aligned}$$

et

$$\begin{aligned} \mu \cdot \alpha + \mu\alpha' &= (ax + 3by;\ ay + bx) + (a'x + 3b'y;\ a'y + b'x) \\ &= (ax + 3by + a'x + 3b'y;\ ay + bx + a'y + b'x). \end{aligned}$$

Donc :

$\boxed{D}$ $\qquad (\forall\alpha)(\forall\alpha')(\forall\mu) \qquad \mu(\alpha + \alpha') = \mu \cdot \alpha + \mu\alpha'.$

En conséquence :

F est un corps commutatif.

4° L'application φ est manifestement une *bijection*.

De plus :

$$\varphi\,(\alpha + \alpha') = \varphi\,[a + a' + (b + b')\sqrt{3}] = (a + a'; b + b')$$

et

$$\begin{aligned} \varphi\,(\alpha) + \varphi\,(\alpha') &= \varphi\,(a + b\sqrt{3}) + \varphi\,(a' + b'\sqrt{3}) \\ &= (a; b) + (a'; b') \\ &= (a + a'; b + b'). \end{aligned}$$

Donc :

$$\varphi(\alpha + \alpha') = \varphi(\alpha) + \varphi(\alpha')$$

$$\varphi(\alpha\alpha') = \varphi[aa' + 3bb' + (ab' + ba')\sqrt{3}] = (aa' + 3bb'; ab' + ba')$$

et

$$\begin{aligned}\varphi(\alpha)\cdot\varphi(\alpha') &= \varphi(a + b\sqrt{3}) \times \varphi(a' + b'\sqrt{3}) \\ &\doteq (a; b) \times (a'; b') \\ &= (aa' + 3bb'; ab' + ba').\end{aligned}$$

Donc :

$$\varphi(\alpha\cdot\alpha') = \varphi(\alpha)\cdot\varphi(\alpha').$$

Finalement :

*φ **est un isomorphisme de E sur F.***

Les corps E et F sont isomorphes.

519. Problème 4.

a, b, a′, b′, sont quatre nombres naturels. On donne les deux fractions $\frac{a}{b}$ et $\frac{a'}{b'}$, telles que

$$a'b - ab' = 1.$$

1° ***Comparer ces deux fractions.***

2° ***Montrer quelles sont irréductibles.***

3° ***On considère la fraction $\frac{c}{d}$ avec $c = a + a'$ et $d = b + b'$.***

Montrer que $a'd - cb' = 1$ et $cb - ad = 1$.

En déduire que la fraction $\frac{c}{d}$ est irréductible et qu'elle est comprise entre $\frac{a}{b}$ et $\frac{a'}{b'}$.

4° ***Soit n un nombre naturel donné. On définit deux entiers naturels q et q′ par les conditions :***

$$\frac{q}{n} \leqslant \frac{a}{b} < \frac{q+1}{n}$$

$$\frac{q'}{n} \leqslant \frac{a'}{b'} < \frac{q'+1}{n}.$$

Montrer que q et q′ satisfont aux relations :

$$\begin{cases} na = bq + r \\ 0 \leqslant r \leqslant b - 1 \end{cases} \qquad \begin{aligned} na' &= b'q' + r' \\ 0 &\leqslant r' \leqslant b' - 1 \end{aligned}$$

Montrer que

$$q' \geqslant q.$$

Etablir la relation

$$bb'(q' - q) = n + rb' - r'b$$

5° *On suppose que* n *est inférieur à* b + b' *et n'est pas multiple de* b'.

Montrer, en majorant le second membre de la relation précédente que q' = q.

6° *On suppose que* n *est inférieur à* b + b' *et qu'il est multiple de* b'.

Montrer que :

$$\frac{a'}{b'} = \frac{q'}{n}$$

et que

$$q' = q + 1.$$

7° *Déduire de l'étude précédente les deux résultats suivants :*

α) *Entre les fractions* $\frac{a}{b}$ *et* $\frac{a'}{b'}$, *il y a une et une seule fraction de dénominateur égal à* $b + b'$.

β) *Entre les fractions* $\frac{a}{b}$ *et* $\frac{a'}{b'}$, *il n'y a aucune fraction de dénominateur inférieur à* $b + b'$.

8° *Application numérique. Trouver toutes les fractions de dénominateur inférieur ou égal à 25 et comprises entre* $\frac{2}{3}$ *et* $\frac{5}{7}$.

1° En divisant la relation :

$$a'b - ab' = 1 \tag{1}$$

par bb' on obtient :

$$\frac{a'}{b'} - \frac{a}{b} = \frac{1}{bb'}. \tag{2}$$

Donc :

$$\frac{a}{b} < \frac{a'}{b'} \tag{3}$$

2° On utilise la condition de Bezout (cf. 517; 6°).

Etant donnés a et b, il existe deux nombres $u = -b'$ et $v = a'$ tels que $au + bv = 1$; donc a et b sont premiers entre eux; et **la fraction $\frac{a}{b}$ est irréductible.**

On montre de même que ***la fraction*** $\mathbf{\frac{a'}{b'}}$ ***est irréductible.***

3° L'égalité (1) peut s'écrire :

$$a'b + a'b' - a'b' - ab' = 1$$

ou

$$a'(b + b') - b'(a + a') = 1$$

ou

$$a'd - cb' = 1$$

D'après les résultats des n°s 2 et 3, on en déduit que $\frac{c}{d}$ est irréductible et que $\frac{c}{d} < \frac{a'}{b'}$.

On montre de même que : $\frac{a}{b} < \frac{c}{d}$.

On a donc finalement :

$$\mathbf{\frac{a}{b} < \frac{a + a'}{b + b'} < \frac{a'}{b'}}. \qquad (4)$$

4° De la condition :

$$\frac{q}{n} \leqslant \frac{a}{b} < \frac{q+1}{n}$$

on déduit en multipliant par nb :

$$bq \leqslant an < b(q + 1)$$

q est donc le quotient euclidien de an par b; et

$$an = bq + r$$

avec :

$$0 \leqslant r < b$$

ou

$$0 \leqslant r \leqslant b - 1.$$

Donc :

$$\begin{cases} \mathbf{an = bq + r} \\ \mathbf{0 \leqslant r \leqslant b - 1} \end{cases} \qquad (6)$$

De même :

$$\begin{cases} \mathbf{a'n = b'q' + r'} \\ \mathbf{0 \leqslant r' \leqslant b' - 1} \end{cases} \qquad (7)$$

D'autre part des conditions :

$$bq \leqslant an < b(q + 1) \qquad (5)$$

et

$$b'q' \leqslant a'n < b'(q' + 1) \qquad (5')$$

On déduit :

$$\begin{cases} b'(q'+1) > na' \\ \text{et} \\ bq < an \end{cases}$$

ou

$$\begin{cases} q'+1 > \dfrac{na'}{b'} \\ \text{et} \\ q < \dfrac{an}{b} \quad \text{ou} \quad -q > -\dfrac{na}{b} \end{cases}$$

D'où par addition :

$$q'+1-q > n\left(\frac{a'}{b'}-\frac{a}{b}\right).$$

En tenant compte de (2) :

$$q'-q+1 > \frac{n}{bb'}$$

ou

$$q'-q > \frac{n}{bb'}-1$$

ou

$$q'-q > -1$$

ou

$$q'-q \geqslant 0$$

ou

$$\mathbf{q' \geqslant q.} \tag{8}$$

En multipliant (6) par b', et (7) par b, on obtient :

$$nab' = bb'q + rb'$$
$$na'b = bb'q' + r'b.$$

D'où par soustraction

$$n(a'b-ab') = bb'(q'-q) + r'b - rb'$$

Or : $a'b - ab' = 1$; donc :

$$\mathbf{bb'(q'-q) = n + rb' - r'b.} \tag{9}$$

5° *On suppose que* n *est inférieur à* b + b' *et que* n *n'est pas multiple de* b'.

a' et b' étant premiers entre eux, a' n'est pas multiple de b'; et na' n'est pas multiple de b'.

Comme n n'est pas multiple de b', $r' = na' - b'q'$ n'est pas un multiple de b', autrement dit

$$r' \neq 0.$$

Par suite :

$$0 \leqslant r' \leqslant b'-1$$

implique

$$\mathbf{1 \leqslant r' \leqslant b' - 1.} \qquad (10)$$

D'autre part :

$$bb'(q' - q) = n + rb' - r'b;$$

en majorant n par $b + b'$, r par $b - 1$, et en minorant r' par 1, on a:

$$bb'(q' - q) < b + b' + b'(b - 1) - b$$

ou

$$bb'(q' - q) < bb'$$

ou

$$q' - q < 1$$

ou

$$q' < q + 1$$

ou

$$q' \leqslant q.$$

Comme d'autre part (cf. formule 8) :

$$q' \geqslant q$$

on déduit :

$$\mathbf{q' = q.} \qquad (11)$$

6° *On suppose que* n *est inférieur à* b + b' *et que* n *est multiple de* b'

On a :

$$n = kb'.$$

D'où :

$$\begin{aligned} r' &= na' - b'q' \\ &= kb'a' - b'q' \\ &= b'(ka' - q') \end{aligned}$$

r' est multiple de b'; comme $r' < b'$, on a donc :

$$\mathbf{r' = 0} \qquad (12)$$

ce qui implique

$$\mathbf{q' = ka'.}$$

La relation :

$$a'n = b'q' + r'$$

s'écrit donc :

$$a'n = b'q'$$

ou

$$\frac{\mathbf{a'}}{\mathbf{b'}} = \frac{\mathbf{q'}}{\mathbf{n}}. \qquad (14)$$

D'autre part :

$$bb'(b' - q) = n + rb' - r'b$$

donne :

$$bb'(q' - q) < b + b' + b'(b - 1)$$

ou

$$bb'(q' - q) < b + bb'.$$

D'où :

$$q' - q < 1 + \frac{1}{b'}.$$

Comme $q' - q \in N$, on a donc :

$$q' - q \leqslant 1.$$

Or on sait que :

$$q' \geqslant q.$$

On peut donc avoir :

$$q' = q + 1$$

ou

$$q' = q.$$

Si on suppose $q' = q$, on a :

$$\frac{q}{n} < \frac{a'}{b'} < \frac{q+1}{n} \quad \text{et} \quad \frac{q}{n} < \frac{a}{b} < \frac{q+1}{n}.$$

D'où :

$$\frac{ka'}{kb'} < \frac{a}{b} < \frac{a'}{b'} < \frac{q+1}{n}$$

ou

$$\frac{a'}{b'} < \frac{a}{b} < \frac{a'}{b'}$$

ce qui implique

$$\frac{a'}{b'} = \frac{a}{b}.$$

Cette égalité étant impossible, on ne peut donc avoir $q' = q$.

Si on suppose $q' = q + 1$, on a :

$$\frac{q}{n} < \frac{a}{b} < \frac{q+1}{n} < \frac{a'}{b'} < \frac{q+2}{n}.$$

Ce qui est possible. Donc :

$$\mathbf{q' = q + 1.} \qquad (15)$$

7° α) D'après le 3°, il existe entre $\frac{a}{b}$ et $\frac{a'}{b'}$ une fraction $\frac{c}{d} = \frac{a+a'}{b+b'}$:

$$\frac{a}{b} < \frac{a+a'}{b+b'} < \frac{a'}{b'}.$$

Cette fraction $\frac{c}{d}$ est la seule; en effet si entre $\frac{a}{b}$ et $\frac{c}{d} = \frac{a + a'}{b + b'}$ existait une fration $\frac{\lambda}{d} = \frac{\lambda}{b + b'}$ on aurait :

$$\frac{a}{b} < \frac{\lambda}{b + b'} < \frac{a + a'}{b + b'}$$

ou $$a(b + b') < \lambda b < b(a + a')$$
ou $$a(b + b') - b(a + a') < \lambda b - b(a + a') < 0$$
ou $$ab' - ba' < [\lambda - (a + a')]\, b < 0$$
ou $$-1 < [\lambda - (a + a')]\, b < 0$$

Or dans Z cette inégalité est impossible pour $\lambda \neq a + a'$.

On montre de même qu'il n'y a pas de fraction $\frac{\mu}{d} = \frac{\mu}{b + b'}$ entre $\frac{a + a'}{b + b'}$ et $\frac{a'}{b'}$.

Autrement dit :

$\mathbf{\frac{a + a'}{b + b'}}$ ***est l'unique fraction de dénominateur*** $\mathbf{b + b'}$ ***comprise entre*** $\mathbf{\frac{a}{b}}$ ***et*** $\mathbf{\frac{a'}{b'}}$.

D'après le n° 3 les fractions $\frac{a}{b}$ et $\frac{c}{d}$, d'une part, et les fractions $\frac{c}{d}$ et $\frac{a'}{b'}$ satisfont à la condition (1).

β) Soit n un nombre inférieur à $b + b'$.

S'il existait une fraction de dénominateur n entre $\frac{a}{b}$ et $\frac{a'}{b'}$, il existerait un nombre naturel λ tel que

$$\frac{a}{b} < \frac{\lambda}{n} < \frac{a'}{b'}$$

ou

$$\frac{na}{b} < \lambda < \frac{na'}{b'}$$

ou

$$q + \frac{r}{b} < \lambda < q' + \frac{r'}{b'}. \qquad (16)$$

Si n *n'est pas multiple de* b', on a : $q' = q$. (Cf. 5°). D'où :

$$q + \frac{r}{b} < \lambda < q + \frac{r'}{b'}$$

et a fortiori on aurait :

$$q < \lambda < q + 1$$

ce qui est impossible dans N.

Si n est multiple de b', on a : $r' = 0$ et $q' = q + 1$. (cf. 6°). D'où :

$$q + \frac{r}{b} < \lambda < q + 1$$

et a fortiori on aurait :

$$q < \lambda < q + 1$$

ce qui est impossible dans N.

Donc :

***Il n'existe pas de fraction, de dénominateur inférieur à* b + b'*, comprise entre* $\frac{a}{b}$ *et* $\frac{a'}{b'}$.**

8° Soient les fractions $\frac{a}{b} = \frac{2}{3}$ et $\frac{a'}{b'} = \frac{5}{7}$.

Elles satisfont à la condition (1) :

$$\begin{aligned} a'b - ab' &= 3 \times 5 - 2 \times 7 \\ &= 1. \end{aligned}$$

On peut donc appliquer à ces fractions les résultats du problème.

Entre $\frac{2}{3}$ et $\frac{5}{7}$ on peut donc intercaler la fraction $\frac{a + a'}{b + b'} = \frac{7}{10}$:

$$\frac{2}{3} < \frac{7}{10} < \frac{5}{7}.$$

Entre $\frac{2}{3}$ et $\frac{7}{10}$, on peut intercaler $\frac{9}{13}$.

Entre $\frac{7}{10}$ et $\frac{5}{7}$, on peut intercaler $\frac{12}{17}$:

$$\frac{2}{3} < \frac{9}{13} < \frac{7}{10} < \frac{12}{17} < \frac{5}{7}.$$

Puis de même, en arrêtant lorsque les dénominateurs trouvés dépassent 25 :

$$\frac{2}{3} < \frac{11}{16} < \frac{9}{13} < \frac{16}{23} < \frac{7}{10} < \frac{12}{17} < \frac{17}{24} < \frac{5}{7}.$$

Et ensuite :

$$\frac{2}{3} < \frac{13}{19} < \frac{11}{16} < \frac{9}{13} < \frac{16}{23} < \frac{7}{10} < \frac{12}{17} < \frac{17}{24} < \frac{5}{7}$$

puis :

$$\frac{2}{3} < \frac{15}{22} < \frac{11}{16} < \frac{9}{13} < \frac{16}{23} < \frac{7}{10} < \frac{12}{17} < \frac{17}{24} < \frac{5}{7}$$

et finalement :

$$\frac{2}{3} < \frac{17}{25} < \frac{15}{22} < \frac{11}{16} < \frac{9}{13} < \frac{16}{23} < \frac{7}{10} < \frac{12}{17} < \frac{17}{24} < \frac{5}{7}.$$

EXERCICES ET PROBLÈMES SUR LE LIVRE III.

Espaces vectoriels.

331. Soient :

$$A = \begin{pmatrix} 2 \\ -1 \end{pmatrix} \qquad B = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

Calculer A + B et A − B.

332. Soient les vecteurs :

$$A = \begin{pmatrix} \sqrt{2} - 1 \\ 1 \end{pmatrix} \qquad B = \begin{pmatrix} \sqrt{2} \\ 3 \end{pmatrix}$$

Calculer A + B et A − B.

333. On donne les matrices :

$$A = \begin{pmatrix} \frac{1}{2} \\ 1 - \frac{\sqrt{2}}{2} \end{pmatrix} \qquad B = \begin{pmatrix} -\frac{1}{2} + \sqrt{2} \\ \sqrt{2} - \frac{3}{2} \end{pmatrix}$$

Calculer A + B et A − B.

334. Soient les matrices à éléments complexes :

$$A = \begin{pmatrix} 3 + 2i \\ 2 - i \end{pmatrix} \qquad B = \begin{pmatrix} -2 + 3i \\ 2i - 3 \end{pmatrix}$$

Calculer A + B et A − B.

335. Soient les matrices à éléments dans K = Z/5.

$$A = \begin{pmatrix} \dot{2} \\ \dot{3} \end{pmatrix} \qquad B = \begin{pmatrix} \dot{1} \\ \dot{2} \end{pmatrix}$$

Calculer A + B et A − B.

336. On donne les matrices :

$$A = \begin{pmatrix} 2i \\ 3 - i \\ 4 \end{pmatrix} \qquad B = \begin{pmatrix} -i \\ 2 + i \\ 4 \end{pmatrix}$$

Calculer $A + B$ et $A - B$.

337. Soient :

$$A = \begin{pmatrix} -\frac{2}{3} \\ \frac{1}{3} \\ 2 \end{pmatrix} \qquad B = \begin{pmatrix} -1 \\ 2 \\ -\frac{1}{3} \end{pmatrix}$$

Calculer $A + B$ et $A - B$.

338. On donne :

$$A = \begin{pmatrix} 2 \\ 1 - i \end{pmatrix} \qquad B = \begin{pmatrix} -1 \\ 1 \end{pmatrix} \qquad C = \begin{pmatrix} i \\ -1 \end{pmatrix}$$

Calculer $A + B + C$ et $A - B - C$.

339. Soient dans $Z/6$ les matrices :

$$A = \begin{pmatrix} \dot{2} \\ \dot{1} \\ \dot{0} \end{pmatrix} \qquad B = \begin{pmatrix} \dot{4} \\ \dot{2} \\ \dot{1} \end{pmatrix} \qquad C = \begin{pmatrix} \dot{0} \\ \dot{3} \\ \dot{2} \end{pmatrix}$$

Calculer $A + B + C$ et $A - B + C$.

340. Dans l'espace vectoriel R^2, on donne les vecteurs

$$X = (2; 3) \qquad Y = (-3; 2) \qquad Z = (4; -5).$$

Calculer $X + Y + Z$ et $X - Y - Z$.

341. Dans l'espace R^3 on considère :

$$X = (1; 2; 3) \qquad Y = (2; 3; 1) \qquad Z = (3; 2; 1).$$

Calculer $X + Y - Z$ et $Y - Z - X$.

342. Dans l'espace vectoriel C^3 on a les vecteurs :

$$X = (1 + i; 1 - i; 2); \qquad Y = (1; -i; i); \qquad Z = (1 - i; 1 + i; 1 + i).$$

Calculer $-X + Y - Z$ et $X + Z - Y$.

343. Soit l'anneau $A = Z/6$. Dans A^3, on donne :

$$X = (\dot{2}; \dot{3}; -\dot{1}) \quad Y = (\dot{4}; \dot{3}; \dot{1}) \quad Z = (\dot{0}; \dot{1}; \dot{0})$$

Calculer $X + Y$; $X - Y + Z$ et $Y - X + Z$.

344. Dans R^3, on donne :

$$X = (2; -5; 3)$$

Calculer $3X$ et $-2X$.

345. Dans R^3, on donne :

$$X = (\sqrt{2} - 1; \sqrt{2} + 1; -1) \qquad Y = (\sqrt{2} - 1; \sqrt{2}; -\sqrt{2} + 1).$$

Calculer $(3 - \sqrt{2})X + (\sqrt{2} + 1)Y$.

346. Dans K^3 avec $K = Z/7$, on considère :

$$X = (\dot{2}; -\dot{1}; \dot{4}) \qquad Y = (\dot{1}; \dot{3}; \dot{0}) \qquad Z = (\dot{3}; \dot{0}; -\dot{2}).$$

Calculer $\quad \dot{2} \cdot X - \dot{3} \cdot Y + \dot{4} \cdot Z.$

347. Soient les matrices à éléments complexes :

$$A = \begin{pmatrix} 2-i \\ 3+i \\ i \end{pmatrix} \qquad B = \begin{pmatrix} 1-i \\ 1+2i \\ -1 \end{pmatrix} \qquad C = \begin{pmatrix} 2-3i \\ 4-5i \\ 3+2i \end{pmatrix}$$

et les nombres $\alpha = i$, $\beta = 1 - i$, $\gamma = 2 + 3i$.

Calculer :

$$\alpha A + \beta B + \gamma C.$$

348. Soient les vecteurs :

$$A = \begin{pmatrix} 2 \\ 2 \end{pmatrix} \qquad B = \begin{pmatrix} 4 \\ -1 \end{pmatrix}$$

Calculer Det (A; B).

349. Soient dans R^3 les vecteurs :

$$A = (1; 1; -2) \qquad B = (2; -1; 4) \qquad C = (2; -1; 6)$$

Calculer Det (A; B; C).

350. Soient dans R^3 les vecteurs

$$A = (7^4 - 2; 4) \qquad B = (5; -1; 0) \qquad C = (8; 0; 1)$$

Calculer Det (A; B; C).

351. Calculer les déterminants :

$$\begin{vmatrix} \frac{1}{3} & \frac{1}{2} \\ \frac{1}{6} & -\frac{1}{4} \end{vmatrix} \qquad \begin{vmatrix} 1 & 1 & -6 \\ 1 & -1 & 4 \\ -2 & 3 & -1 \end{vmatrix}$$

352. Calculer :

$$D = \begin{vmatrix} 1 & 0 & 6 \\ 1 & 2 & 0 \\ 1 & -5 & -7 \end{vmatrix} \qquad \Delta = \begin{vmatrix} -5 & 0 & 2 \\ -7 & 6 & 0 \\ -2 & 1 & -3 \end{vmatrix}$$

353. Calculer :

$$D = \begin{vmatrix} 1+i & 2+3i \\ 1-i & 3-2i \end{vmatrix} \qquad D' = \begin{vmatrix} 5-3i & 3-2i \\ 3+5i & 3+2i \end{vmatrix}$$

354. Calculer les déterminants :

$$A = \begin{vmatrix} 3-i & 2i & 1 \\ -2 & 3i-1 & 0 \\ 1+i & 0 & 3-2i \end{vmatrix} \qquad B = \begin{vmatrix} 2i-3 & 5i & i \\ 4 & 0 & -3 \\ 2+3i & 3-2i & 0 \end{vmatrix}$$

355. Dans K^2 avec $K = Z/5$, calculer les déterminants :

$$D = \begin{vmatrix} \dot{2} & \dot{4} \\ -\dot{3} & \dot{3} \end{vmatrix} \qquad D' = \begin{vmatrix} -\dot{1} & \dot{3} \\ \dot{0} & \dot{4} \end{vmatrix}$$

356. Dans A^3 avec $A = Z/6$, calculer les déterminants :

$$D = \begin{vmatrix} \dot{2} & \dot{3} & \dot{0} \\ -\dot{1} & \dot{4} & \dot{5} \\ \dot{0} & \dot{2} & \dot{1} \end{vmatrix} \qquad D' = \begin{vmatrix} \dot{4} & \dot{5} & -\dot{1} \\ -\dot{2} & -\dot{3} & \dot{4} \\ \dot{1} & \dot{3} & -\dot{4} \end{vmatrix}$$

Indépendance linéaire. Bases.

Etudier la dépendance des vecteurs suivants :

357. $A = (m - 1 ; 3)$ $B = (m + 1 ; - 1)$.

358. $A = (6 ; 4 - m)$ $B = (m + 1 ; 3m + 1)$.

359. $A = (1 ; 1 ; 4)$ $B = (1 ; - 1 ; 2)$ $C = (1 ; 1 ; 1)$.

360. $A = (1 ; 5 ; a)$ $B = (1 ; a ; 4)$ $C = (1 ; 3 ; 5)$.

361. $A = \begin{pmatrix} 1 \\ m \\ 1 \end{pmatrix}$ $B = \begin{pmatrix} m \\ 1 \\ m \end{pmatrix}$ $C = \begin{pmatrix} m + 1 \\ 1 \\ 1 \end{pmatrix}$

362. $U = \begin{pmatrix} - 3m \\ 1 - m \\ - m \end{pmatrix}$ $V = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}$ $W = \begin{pmatrix} 5 \\ 4 \\ 9 \end{pmatrix}$

363. $A = (2 + i ; 1 - i)$ $B = (1 - i ; 4 + i)$.

364. $A = (1 - i ; 2 + i ; - 1)$ $B = (- 1 ; 2 - i ; 1 - i)$ $C = (2 - i ; - 1 ; 2 + i)$

Les systèmes de vecteurs suivants constituent-ils des bases :

365. $u = (\sqrt{2} ; - 1)$ $v = (1 ; \sqrt{2})$.

366. $u = (2 + i ; 1 - i)$ $v = (4 + i ; 2 + 3i)$.

367. $A = \begin{pmatrix} a \\ a - 1 \end{pmatrix}$ $B = \begin{pmatrix} 2 + 3a \\ a - 4 \end{pmatrix}$

368. $A = \begin{pmatrix} 2 \\ 3 \\ 3 \end{pmatrix}$ $B = \begin{pmatrix} 6 \\ - 1 \\ 2 \end{pmatrix}$ $C = \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}$

369. $A = (1 ; 1 ; 2)$ $B = \left(\frac{21}{5} ; - \frac{14}{3} ; \frac{7}{2}\right)$ $C = \left(- 3 ; 1 ; - \frac{9}{4}\right)$

370. $A = \begin{pmatrix} 1 + i \\ i \\ 1 + 2i \end{pmatrix}$ $B = \begin{pmatrix} \frac{3}{5}i \\ 1 - \frac{2}{3}i \\ 1 + \frac{1}{2}i \end{pmatrix}$ $C = \begin{pmatrix} 1 - 3i \\ 1 + i \\ - \frac{9i}{4} \end{pmatrix}$

371. $A = (5 - 2i ; - 2 + i ; 3 + i)$
$B = (- 5 + i ; 2 - 2i ; - 3 + i)$
$C = (1 + i ; i ; 4 - 2i)$.

372. $A = (1 - i ; 2 + 2i ; 3 + 2i)$
$B = (2 + 2i ; 3 - i ; 2 + 2i)$
$C = (3 + 2i ; 2 + i ; 1 - i)$.

373. $X = \begin{pmatrix} 1 \\ a \\ b + c \end{pmatrix}$ $Y = \begin{pmatrix} 1 \\ b \\ c + a \end{pmatrix}$ $Z = \begin{pmatrix} 1 \\ c \\ a + b \end{pmatrix}$

374. Soit le vecteur de R^3

$$U = (5; 4; 6)$$

Donner les coordonnées du vecteur $X = t \cdot U$ ($t \in R$) en fonction de t.

375. Etudier la famille de vecteurs :

$$\{ X = tU \ / \ U = (-1; -1; 1) \}$$

376. Etudier l'ensemble des vecteurs $t \cdot U$ avec $U = (2; 3; 4)$.

377. Soit le vecteur :

$$X = (\dot{1}; \dot{2}; -\dot{2}),$$

dont les éléments appartiennent à $K = Z/5$. Etudier la famille $t \cdot X$, $t \in K$.

378. Dans R^2, on considère les vecteurs :

$$u = (1; 7) \qquad v = (1; 3)$$

Montrer que $\mathcal{B} = \{ u; v \}$ est une base.

Soit X =' (5; 7). Calculer les coordonnées de X dans la base $\mathcal{B}$.

379. Montrer que dans R^2, les vecteurs $j = (0; 1)$ et $u = (5; 7)$ constituent une base $\mathcal{B}$.

On donne $U = (7; 3)$ dans la base canonique $B = \{ i; j \}$. Donner les formules de changement de base. Quelles sont les coordonnées de U dans la base $\mathcal{B}$.

380. Dans R^3, on considère les vecteurs :

$$u = (1; 0; 1) \qquad v = (1; 1; 0) \qquad w = (0; 1; 1)$$

Montrer que $\mathcal{B} = \{ u; v; w \}$ est une base.

Soit dans la base canonique le vecteur $U = (2; 2; 2)$. Trouver les coordonnées de U dans $\mathcal{B}$.

Soit dans la base $\mathcal{B}$ le vecteur $V = (2; 2; 2)$. Trouver les coordonnées de V dans $\mathcal{B}_0$.

381. Montrer que les trois vecteurs :

$$u = \begin{pmatrix} 1 \\ 4 \\ 5 \end{pmatrix} \qquad v = \begin{pmatrix} 1 \\ 6 \\ 6 \end{pmatrix} \qquad w = \begin{pmatrix} 1 \\ 9 \\ 7 \end{pmatrix}$$

forment une base $\mathcal{B}$. Est-ce une base positive ?

Donner les formules de changement de base.

Soit le vecteur U donné dans la base canonique $\mathcal{B}_0$.

$$U = \begin{pmatrix} 1 \\ 6 \\ 7 \end{pmatrix}$$

Quelles sont les coordonnées de ce vecteur dans la base $\mathcal{B}$?

Soit le vecteur V donné dans la base $\mathcal{B}$:

$$V = \begin{pmatrix} 5 \\ 6 \\ 1 \end{pmatrix}$$

Quelles sont les coordonnées de ce vecteur dans la base canonique $\mathcal{B}_0$.

Espaces vectoriels métriques.

Calculer le produit scalaire euclidien des vecteurs suivants :

382. $u = (1; 1)$ $\qquad$ $v = (7; 3)$

383. $u = (45; 37)$ $\qquad$ $v = (45; 17)$

384. $u = (28; 29)$ $v = (30; 31)$

385. $u = (1; -1; -1)$ $v = (-1; -1; 1)$

386. $u = (1; 1; 1)$ $v = (2; 3; 4)$

387. $u = (1; a; a^2)$ $v = (a^2; 1; a)$

388. $u = (6; 4; 3)$ $v = (7; 8 - 7)$

389. $u = \left(\frac{2}{3}; \frac{2}{3}; \frac{1}{3}\right)$ $v = \left(-\frac{2}{3}; \frac{1}{3}; \frac{2}{3}\right)$

390. $u = (0; 1; 5; 9)$ $v = (2; 1; 6; 8)$

Évaluer la norme des vecteurs suivants :

391. $A = (2; 4)$ $B = (3; -2)$ $C = \left(\frac{\sqrt{2}}{1}; -\frac{\sqrt{2}}{1}\right)$

392. $u = (4; 1)$ $v = (-1; 3)$ $w = (\sqrt{2} - 1; \sqrt{3} + 1)$

393. $u = (4; -7; 11)$ $v = (-6; 4; 3)$ $w = (3; -1; -2)$

394. $u = \left(\frac{2}{3}; \frac{2}{3}; \frac{1}{3}\right)$ $v = \left(\frac{1}{3}; -\frac{2}{3}; \frac{2}{3}\right)$

Donner les coordonnées du vecteur unitaire associé aux vecteurs suivants :

395. $u = (3; 2)$ $v = (-4; -3)$

396. $u = (12; -5)$ $v = (-7; 6)$

397. $u = (1; 2; 3)$ $v = (2; -1; 1)$ $w = (1; 0; 1)$

398. $u = (-2; 1; 3)$ $v = (-3; 2; 3)$ $w = (-1; 1; 2)$

399. $u = (-2; -3; -1)$ $v = (1; 2; 1)$ $w = (3; 3; 2)$

400. $u = (2; -2; 1; -1)$ $v = (1; 2; -2; -1)$ $w = (1; 3; -2; 0)$

Vérifier si les vecteurs suivants sont orthogonaux :

401. $u = (1; 2)$ $v = (2; -1)$

402. $u = (2; 3)$ $v = \left(1; -\frac{2}{3}\right)$

403. $u = (2; 3; -1)$ $v = (1; 2; 8)$

404. $u = (2; 2; 1)$ $v = (2; -1; -2)$

405. $u = (9; 6; -2)$ $v = (6; -6; 9)$

406. Soient les vecteurs :

$$u = (2; 1) \qquad v = (1; 1)$$

Montrer qu'ils sont linéairement indépendants.
Trouver un vecteur u' orthogonal à u, et un vecteur v' orthogonal à v.

407. Soient les vecteurs :

$$u = (2; 1; -3) \quad \text{et} \quad v = (1; 2; 1)$$

On pose :

$$U = u + \lambda v.$$

Déterminer λ pour que U soit orthogonal à u.

408. On donne les vecteurs :

$$u = (2; 6; -3) \qquad v = (6; 0; 1) \qquad w = (1; 1; 1)$$

On pose :

$$U = u + \lambda v.$$

Déterminer λ pour que U soit orthogonal à u.

On pose alors :

$$V = u + xU + yw$$

Peut-on déterminer x et y pour V soit orthogonal à u; v et U.
Donner une base $\mathcal{B}$ orthonormée de l'espace R^3.

409. Soient les vecteurs de R^2

$$A = (3; 4) \qquad B = (-5; 10)$$

Calculer : $\|A\|$, $\|B\|$ et $\|A - B\|$.

410. On considère les vecteurs :

$$u = (9; 6; -2) \qquad v = (7; -4; 9)$$

Calculer : $\|u\|$, $\|v\|$, $\|u - v\|$ et $u \cdot v$.

411. On donne dans R^3 les vecteurs :

$$A = (-8; 2; -5) \qquad B = (-2; 12; 10) \qquad C = (10; 8; -4)$$

Calculer :

$$\|A\|; \ \|B\|; \ \|C\|.$$
$$\|A - B\|; \ \|B - C\|; \ \|C - A\|$$

412. On donne les vecteurs :

$$u = (4; 5; -2) \qquad v = (0; -3; 6)$$

Calculer le cosinus du bivecteur $\{u; v\}$.
Calculer les cosinus des deux bivecteurs $\{u; u + v\}$ et $\{v; u + v\}$

413. On donne les vecteurs :

$$u = (-3; -3) \qquad v = (1; 1)$$

Calculer sin $(u; v)$ et cos $(u; v)$.

414. Soient les vecteurs :

$$u = (-6; -2) \qquad v = (-4; 2) \qquad w = (0; -2)$$

Calculer le sinus et le cosinus du bivecteur $\{v - u; w - u\}$.

415. Calculer le sinus et le cosinus du bivecteur (U; V) avec

$$U = (-8; -6) \qquad V = (4; 3)$$

416. On donne les vecteurs de R^2 :

$$A = (-4; 2) \qquad B = (4; 3) \qquad C = (-1; 4)$$

Calculer les sinus et les cosinus des bivecteurs suivants :

$$(B - A; C - A) \qquad (C - B; A - B) \qquad (A - C; B - C)$$

417. On donne :

$$u = (2; -1; 2) \qquad v = (4; 0; -3)$$

Calculer le cosinus des bivecteurs $(u; v)$.

418. Calculer le produit vectoriel des vecteurs

$$u = (1; 1; 0) \qquad v = (3; 2; 1).$$

419. Calculer $u \wedge v$ sachant que $u = (2; -1; 0) \qquad v = (-1; 2; -1)$.

420. On donne :

$$A = (1; 1; 0) \quad \text{et} \quad B = (1; 0; 2)$$

Calculer la norme du vecteur $B - A$.
Calculer le cosinus du bivecteur $(A; B)$.
Calculer $A \wedge B$.

421. On donne les vecteurs u et v; calculer $u \wedge v$.
a) $u = (1; 2; 2) \qquad v = (-1; 0; 2)$
b) $u = (2; 2; 3) \qquad v = (1; 0; 3)$
c) $u = (2; 1; 2) \qquad v = (2; -5; 14)$

422. On donne :

$$a = (-2; 3; 4) \qquad b = (1; -2; 0)$$

Calculer le sinus et le cosinus du bivecteur $(a; b)$.

423. Soient les vecteurs

$$u = (1; 8; 4) \quad \text{et} \quad v = (2; -2; -1)$$

Calculer $\sin(u; v)$ et $\cos(u; v)$.

424. Calculer le produit mixte des trois vecteurs :

$$u = (3; 2; 1) \qquad v = (5; 2; 2) \qquad w = (4; 1; 2)$$

425. On donne :

$$A = (1; -5; 2) \qquad B = (4; -2; 1) \qquad C = (-3; 1; 2)$$

Calculer le produit mixte $(A \wedge B) \cdot C$.

426. On donne :

$$u = (3; 4; 0) \qquad v = (0; 3; 4)$$

Déterminer l'ensemble des vecteurs orthogonaux à la fois aux deux vecteurs u et v.

427. Soit le vecteur $u = (1; -1; 1)$. Déterminer la variété linéaire orthogonale au vecteur u.

428. On considère les vecteurs

$$a = (-1; -2; 4) \qquad b = (2; 3; -1).$$

Déterminer la variété linéaire orthogonale aux vecteurs a et b.

429. Dans l'espace vectoriel R^4 on considère les vecteurs :

$$u = (-1; 0; 1; 2) \quad \text{et} \quad v = (3; 2; -1; -2)$$

Déterminer la variété orthogonale aux deux vecteurs u et v.

430. On considère dans R^3 les vecteurs :

$$u = \left(\frac{2}{3}; -\frac{2}{3}; \frac{1}{3}\right) \qquad = \left(\frac{2}{3}; \frac{1}{3}; -\frac{2}{3}\right) \qquad w = \left(\frac{1}{3}; \frac{2}{3}; \frac{2}{3}\right)$$

1° Montrer que $\mathcal{B} = \{ u; v; w \}$ est une base orthonormée.

2° Calculer Det $(u; v; w)$.

3° On considère le vecteur $\Omega = \left(\frac{1}{\sqrt{2}}; 0; \frac{1}{\sqrt{2}}\right)$. Calculer $\|\Omega\|$.

4° Calculer $\cos(j; v)$.

5° Calculer les produits scalaires $\Omega \cdot j$ et $\Omega \cdot v$.

Polynômes et fractions.

431. On donne :

$A = (1; 2; 2; 1; 0; 0; ...)$ et $B = (-1; 2; -2; 1; 0; 0; ...)$

Calculer $A + B$, $A - B$, AB.

432. Soient les polynômes :

$A = (1; -3; 3; -1; 0; 0; ...)$ et $B = (1; -2; 1; 0; 0; ...)$

Calculer $A + B$ et AB.

433. On donne les polynômes formels :

$A = (-12; 7; -5; -3; 0; 0; ...)$ et $B = (9; -6; 4; -2; 0; 0; ...)$

Calculer $2A - 3B$ et $A - 2B$.

434. On considère les polynômes formels :

$A = (11; 10; -4; 0; 0 ...)$ et $B = (13; -10; -1; 0; 0 ...)$

Calculer $-A + 3B$, $A - B$ et $(A - B) \cdot (3B - A)$

435. Soient les polynômes

$A = (-24; 16; -11; 14; 0; 0 ...)$ et $B = (-18; 12; -8; -7; 0; 0 ...)$

Exprimer ces polynômes dans la base canonique. Calculer ensuite $A + B$ et $2A - 3B$.

436. Soient :

$A = (-2; 7; -4; -5; 3; 0; 0; ...)$ et $B = (4; -3; -5; 2; 0; 0; ...)$

Exprimer A et B en fonction du polynôme u; puis calculer AB.

437. Calculer :

$$(3 - 5u + 7u^2)(1 + 4u) + (2 - 8u + 3u^2)(1 - 4u)$$

438. Calculer :

$$(1 + 2u + 2u^2 + u^3)(1 - 2u + 2u^2 - u^3)$$

439. Calculer :

$$(u^3 - 2u + 1)(u^2 - u + 1)$$

440. Effectuer les divisions suivantes

1° $4u^2 - 78u + 580 : 2x - 13$.

2° $u^2 - 11u + 37 : u - 7$.

441. Effectuer les divisions suivantes :

1° $10u^4 - 16u^3 - 39u^2 + 2u + 15 : -5u^2 - 2u + 3$.

2° $15u^4 - 22u^3 + 16u^2 - 6u + 1 : 3u^2 - 2u + 1$.

442. Calculer :

$$144u^8 - 520u^6 + 497u^4 - 130u^2 + 9 : 18u^3 - 9u^2 - 2u + 1.$$

443. Calculer :

1° $(3u^4 - 5u^3v - 4u^2v^2 + 7uv^3 - 2v^4)(2u^3 - 5u^2v - 3uv^2 + 4v^3).$

2° $(4u^3 - 3u^2v + 2uv^2 - 7v^3)(5u^2 + 2uv - v^2).$

444. Effectuer :

1° $(u^n - 3u^{n-1}v + 4u^{n-2}v^2 - 6u^{n-3}v^3 + 5u^{n-4}v^4)(2u^3 - u^2v + uv^2)$

2° $(u^{n+2} + 2u^{n+1}v - 3u^nv^2)(u^n - 2u^{n-1}v + 3u^{n-2}v^2)$

445. Simplifier les fractions :

$$\frac{12u^2 - 12}{36u^3 - 36}; \quad \frac{4u^2 + 12u}{6u^3 - 54u}; \quad \frac{12u^2 - 27}{6u + 9}.$$

446. Décomposer en produit les polynômes suivants :

$$A = 10 - 7u + 10u^2 - 7u^3 \qquad B = 1 - 2u + u^2 - 2u^3$$

Puis simplifier la fraction $\frac{A}{B}$.

447. Décomposer :

$$A = 6u^2 - 13uv + 6v^2 \quad \text{et} \quad B = 4u^2 - 9v^2$$

Simplifier la fraction $\frac{A}{B}$.

448. Calculer le P.G.C.D. des polynômes :

$$A = 4u^2 + 3uv - v^2 \quad \text{et} \quad B = 5u^2 + 4uv - v^2.$$

Simplifier la fraction $\frac{A}{B}$.

449. Calculer le P.G.C.D. des polynômes :

$$A = 10u^2 - 21uv - 10v^2 \quad \text{et} \quad B = 4u^2 - 25v^2.$$

Simplifier $\frac{A}{B}$.

450. Calculer le P.P.C.M. des polynômes :

$$A = 2u + 2 \qquad B = 3u - 3 \qquad C = 6u^2 - 6.$$

Puis calculer :

$$\frac{3}{2u + 2} - \frac{2}{3u - 3} + \frac{5u + 3}{6u^2 - 6}.$$

451. Calculer :

$$\frac{64}{u^2 - 16} + \frac{u - 4}{u + 4} - \frac{u + 4}{u - 4}.$$

452. Calculer :

$$\frac{3}{u - 1} - \frac{4u - 1}{u + 1} - \frac{u^2 + 5}{u^2 - 1} + 5.$$

453. Calculer :

$$\frac{15 - 8u - 4u^2}{1 - u^2} + \frac{4 + 9u}{1 + u} - \frac{3 - 7u}{1 - u} - 6.$$

454. Calculer :
$$\frac{15}{3u-2v} - \frac{4}{3(u-v)} - \frac{5(3u-v)}{(3u-3v)(3u-2v)}.$$

455. Calculer :
$$\frac{u+2}{2v-u} + \frac{u-2}{2v+u} - \frac{4v}{4v^2-u^2}.$$

456. Calculer :
$$\frac{3u-v}{3u+v} - \frac{2u-v}{2u+v} - \frac{u-v}{u+v} - 1.$$

Exercices divers.

457. Démontrer que :
$$\left(\frac{a}{a'} + \frac{b'}{b} = 1 \quad \text{et} \quad \frac{b}{b'} + \frac{c'}{c} = 1\right) \Rightarrow (abc + a'b'c' = 0).$$

458. Si $2p = a + b + c$, calculer :
$$(p-a)^2 + (p-b)^2 + (p-c)^2.$$

459. Démontrer l'équivalence :
$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow \frac{a+b}{a-b} = \frac{c+d}{c-d}.$$

460. Démontrer l'identité :
$$x(x+1)(x+2)(x+3) + 1 = (x^2+3x+1)^2$$
Que peut-on en conclure si x est un entier naturel ?

461. Montrer que :
$$(a+b+c)^3 = \Sigma a^3 + \Sigma 3a^2b + 6abc$$
En déduire :
$$(a+b+c)^3 - (b+c-a)^3 - (c+a-b)^3 - (a+b-c)^3$$

462. Sachant que :
$$r^2 = (x-c)^2 + y^2 \qquad \text{et} \qquad r'^2 = (x+c)^2 + y^2$$
calculer le produit :
$$(r+r'+2a)(r+r'-2a)(r-r'+2a)(r-r'-2a)$$

463. On donne :
$$4\alpha^2 = 2(b^2+c^2) - a^2 \qquad 4\beta^2 = 2(c^2+a^2) - b^2 \qquad 4\gamma^2 = 2(a^2+b^2) - c^2$$
Calculer :
$$\alpha^2 + \beta^2 + \gamma^2;$$
$$\alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2;$$
$$\alpha^4 + \beta^4 + \gamma^4$$
en fonction de a, b, c.

464. Calculer les expressions suivantes de a, b, c :

1° $\displaystyle\sum \frac{1}{(a-b)(a-c)}.$

2° $\displaystyle\sum \frac{a}{(a-b)(a-c)}.$

3° $\sum \frac{b+c}{(a-b)(a-c)}$.

4° $\sum \frac{a^3}{(a-b)(a-c)}$.

465. Montrer que :

$$\sum \frac{4a^2-1}{(a-b)(a-c)}$$

ne dépend pas de a, b, c. Quelle est la valeur de cette somme ?

466. Soient trois nombres distincts a, b, c. Démontrer l'implication

$$\left(\sum \frac{a}{b-c} = 0\right) \Rightarrow \left(\sum \frac{a}{(b-c)^2} = 0\right)$$

467. On sait que $a + b + c = 0$, calculer alors :

$$x = \left(\sum \frac{a}{a-c}\right) \cdot \left(\sum \frac{b-c}{a}\right).$$

468. Calculer :

$$\frac{b+c}{bc}(b^2+c^2-a^2) + \frac{c+a}{ca}(c^2+a^2-b^2) + \frac{a+b}{ab}(a^2+b^2-c^2).$$

469. Calculer, en fonction de a, b, c :

$$x = \sum \frac{a^2b^2}{(a-c)(b-c)}.$$

470. Montrer que les deux assertions :

α) $bc\,(y-z)^2 + ca\,(z-x)^2 + ab\,(x-y)^2 = (a+b+c)\,(ax^2+by^2+cz^2)$

β) $ax + by + cz = 0$

sont équivalentes.

471. Démontrer que la différence des cubes de deux nombres entiers consécutifs est égale au carré d'un nombre entier augmenté du triple du carré d'un autre nombre entier.

472. Si y, z et t désignent trois nombres entiers et si le nombre entier $y^2 + 2tz^2$ est le carré d'un nombre entier, le nombre entier $y^2 + tz^2$ est la somme des carrés de deux nombres entiers.

473. Démontrer que la somme de deux fractions irréductibles, de dénominateurs différents, n'est jamais un nombre entier.

474. Si α, β, γ sont trois nombres distincts satisfaisant aux relations

$$\alpha^3 + p\alpha + q = 0$$
$$\beta^3 + p\beta + q = 0$$
$$\gamma^3 + p\gamma + q = 0$$

prouver que l'on doit avoir $\alpha + \beta + \gamma = 0$.

475. Décomposer en un produit :

$$2x^2y^2 + 2y^2z^2 + 2z^2x^2 - x^4 - y^4 - z^4.$$

476. Simplifier :

$$\frac{ab(x^2+y^2) + xy(a^2+b^2)}{ab(x^2-y^2) + xy(a^2-b^2)}$$

a, b sont des constantes; x et y des indéterminées.

477. Démontrer :

$$[a \in R_+ \text{ et } b \in R_+] \Rightarrow \left[(a+b)\left(\frac{1}{a}+\frac{1}{b}\right) > 4\right]$$

et

$$[a \in R_+ \text{ et } b \in R_+] \Rightarrow [a^3 + b^3 > a^2b + ab^2].$$

478. Calculer, dans le corps C,

$$(2+3i)^2 + (2-3i)^2$$
$$(1+2i)^4 + (1-2i)^4$$
$$\frac{2+3i}{1+2i} + \frac{2-3i}{1-2i}.$$

479. On donne le nombre complexe :

$$j = -\frac{1}{2} + \frac{\sqrt{3}}{2} \cdot i.$$

Calculer j^2, j^3 et $1 + j + j^2$.

480. Si a et b sont des nombres complexes, montrer que l'on a :

$$a^3 + b^3 = (a+b)(aj + bj^2)(aj^2 + bj)$$

481. Dans le corps C, on considère les nombres :

$$x = a + b + c \qquad y = a + bj + cj^2 \qquad z = a + bj^2 + cj$$

Calculer $x^3 + y^3 + z^3$.

482. Soit le polynôme :

$$A = z^2 - 2iz + 2(1+i)$$

avec $z = x + iy$

Mettre A sous la forme $A = X + iY$ $(X \in R;\ Y \in R)$

483. 1° Montrer que l'ensemble des polynômes à coefficients réels et de degré inférieur ou égal à 2 est un espace vectoriel E sur le corps R.

2° Montrer que $\mathcal{B}_0 = \{1; u; u^2\}$ est la base canonique de E.

3° $\mathcal{B} = \{1; 1+u; 1+u^2\}$ est-il une base de E. Pourquoi ?

4° Soit le polynôme :

$$A = 2 + u + 2u^2$$

Peut-on exprimer A en fonction des éléments de $\mathcal{B}$?

484. 1° Montrer que l'ensemble C des nombres complexes est un espace vectoriel de dimension 2 sur le corps des réels.
Montrer que $\mathcal{B}_0 = \{1; i\}$ est une base.

2° Montrer que $\mathcal{B}\{1+i; -1+i\}$ est une autre base de C.

3° Exprimer les nombres $a = 2 - 3i$, $b = 3 - 2i$ dans la base $\mathcal{B}$.

485. Soit le nombre complexe $\alpha = 1 + i$.
Montrer que tout nombre complexe z peut s'écrire de façon unique sous la forme $z = x + y\alpha$, x et y étant des nombres réels.

486. On considère l'ensemble $\mathcal{T}$ des polynômes de degré inférieur ou égal à 1, c'est-à-dire l'ensemble des polynômes de la forme $a + bu$ (a et b réels).

1° Montrer que $\mathcal{T}$ est un espace vectoriel de dimension 2 sur le corps R.

2° Montrer que $\mathcal{T}^2$ est un espace vectoriel. Quelle est sa dimension ? donner une base de cet espace vectoriel.

487. Soit l'espace vectoriel $\mathcal{F}$ des polynômes de la forme $au + b$ (a et b réels). On considère le polynôme $U = 2u - 1$. Etudier l'ensemble E des polynômes $\lambda\,(2u - 1)$. Quelle est la structure de l'ensemble E ?

488. Soient les polynômes :

$$U = u \quad \text{et} \quad V = -1 + u$$

Etudier l'ensemble E formé des polynômes $\lambda U + \mu V$. Quelle est la structure de E.

489. Dans l'espace vectoriel C sur le corps R (cf. ex. 484) on considère les nombres

$$z = 1 + i \quad \text{et} \quad z' = 2 + 3i$$

Montrer qu'il existe une variété affine, de dimension 1, qui contient z et z'

490. On considère l'espace vectoriel $\mathcal{F}$ des polynômes de degré inférieur ou égal à 2 et à coefficients dans R.

1° Montrer que le polynôme $A = 1 + u^2$ appartient à une variété linéaire. Préciser cette variété.

2° On donne $U = 1 + u$ et $V = 1 + u^2$. Montrer que ces deux polynômes déterminent une variété affine et une seule de dimension 1.

3° On donne les polynômes $U = 1 + u$, $V = 1 + u^2$, $W = 1 + u - u^2$. Montrer que ces trois polynômes déterminent une variété affine et une seule de dimension 2.

TABLES DIVERSES

TABLES DIVERSES

Carrés des 100 premiers nombres

Nombres	*Carrés*	*Nombres*	*Carrés*	*Nombres*	*Carrés*	*Nombres*	*Carrés*
1	1	**26**	676	**51**	2 601	**76**	5 776
2	4	**27**	729	**52**	2 704	**77**	5 929
3	9	**28**	784	**53**	2 809	**78**	6 084
4	16	**29**	841	**54**	2 916	**79**	6 241
5	25	**30**	900	**55**	3 025	**80**	6 400
6	36	**31**	961	**56**	3 136	**81**	6 561
7	49	**32**	1 024	**57**	3 249	**82**	6 724
8	64	**33**	1 089	**58**	3 364	**83**	6 889
9	81	**34**	1 156	**59**	3 481	**84**	7 056
10	100	**35**	1 225	**60**	3 600	**85**	7 225
11	121	**36**	1 296	**61**	3 721	**86**	7 396
12	144	**37**	1 369	**62**	3 844	**87**	7 569
13	169	**38**	1 444	**63**	3 969	**88**	7 744
14	196	**39**	1 521	**64**	4 096	**89**	7 921
15	225	**40**	1 600	**65**	4 225	**90**	8 100
16	256	**41**	1 681	**66**	4 356	**91**	8 281
17	289	**42**	1 764	**67**	4 489	**92**	8 464
18	324	**43**	1 849	**68**	4 624	**93**	8 649
19	361	**44**	1 936	**69**	4 761	**94**	8 836
20	400	**45**	2 025	**70**	4 900	**95**	9 025
21	441	**46**	2 116	**71**	5 041	**96**	9 216
22	484	**47**	2 209	**72**	5 184	**97**	9 409
23	529	**48**	2 304	**73**	5 329	**98**	9 604
24	576	**49**	2 401	**74**	5 476	**99**	9 801
25	625	**50**	2 500	**75**	5 625	**100**	10 000

Cubes des 100 premiers nombres

Nombres	Cubes	Nombres	Cubes	Nombres	Cubes	Nombres	Cubes
1	1	**26**	17 576	**51**	132 651	**76**	438 976
2	8	**27**	19 683	**52**	140 608	**77**	456 533
3	27	**28**	21 952	**53**	148 877	**78**	474 552
4	64	**29**	24 389	**54**	157 464	**79**	493 039
5	125	**30**	27 000	**55**	166 375	**80**	512 000
6	216	**31**	29 791	**56**	175 616	**81**	531 441
7	343	**32**	32 768	**57**	185 193	**82**	551 368
8	512	**33**	35 937	**58**	195 112	**83**	571 787
9	729	**34**	39 304	**59**	205 379	**84**	592 704
10	1 000	**35**	42 875	**60**	216 000	**85**	614 125
11	1 331	**36**	46 656	**61**	226 981	**86**	636 056
12	1 728	**37**	50 653	**62**	238 328	**87**	658 503
13	2 197	**38**	54 872	**63**	250 047	**88**	681 472
14	2 744	**39**	59 319	**64**	262 144	**89**	704 969
15	3 375	**40**	64 000	**65**	274 625	**90**	729 000
16	4 096	**41**	68 921	**66**	287 496	**91**	753 571
17	4 913	**42**	74 088	**67**	300 763	**92**	778 688
18	5 832	**43**	79 507	**68**	314 432	**93**	804 357
19	6 859	**44**	85 184	**69**	328 509	**94**	830 584
20	8 000	**45**	91 125	**70**	343 000	**95**	857 375
21	9 261	**46**	97 336	**71**	357 911	**96**	884 736
22	10 648	**47**	103 823	**72**	373 248	**97**	912 673
23	12 167	**48**	110 592	**73**	389 017	**98**	941 192
24	13 824	**49**	117 649	**74**	405 224	**99**	970 299
25	15 625	**50**	125 000	**75**	421 875	**100**	1 000 000

Racines carrées des 100 premiers nombres

Nombres	*Racines carrées*	*Nombres*	*Racines carrées*	*Nombres*	*Racines carrées*	*Nombres*	*Racines carrées*
1	1,000	**26**	5,099	**51**	7,141	**76**	8,718
2	1,414	**27**	5,196	**52**	7,211	**77**	8,775
3	1,732	**28**	5,292	**53**	7,280	**78**	8,332
4	2,000	**29**	5,385	**54**	7,349	**79**	8,888
5	2,236	**30**	5,477	**55**	7,416	**80**	8,944
6	2,450	**31**	5,568	**56**	7,483	**81**	9,000
7	2,646	**32**	5,657	**57**	7,550	**82**	9,055
8	2,828	**33**	5,745	**58**	7,616	**83**	9,110
9	3,000	**34**	5,831	**59**	7,681	**84**	9,165
10	3,162	**35**	5,916	**60**	7,746	**85**	9,220
11	3,317	**36**	6,000	**61**	7,810	**86**	9,274
12	3,464	**37**	6,083	**62**	7,874	**87**	9,327
13	3,606	**38**	6,164	**63**	7,937	**88**	9,381
14	3,741	**39**	6,245	**64**	8,000	**89**	9,434
15	3,873	**40**	6,325	**65**	8,062	**90**	9,487
16	4,000	**41**	6,403	**66**	8,124	**91**	9,539
17	4,123	**42**	6,481	**67**	8,185	**92**	9,591
18	4,243	**43**	6,557	**68**	8,246	**93**	9,644
19	4,359	**44**	6,633	**69**	8,307	**94**	9,695
20	4,472	**45**	6,708	**70**	8,367	**95**	9,747
21	4,583	**46**	6,782	**71**	8,426	**96**	9,798
22	4,690	**47**	6,856	**72**	8,485	**97**	9,849
23	4,796	**48**	6,928	**73**	8,544	**98**	9,900
24	4,899	**49**	7,000	**74**	8,602	**99**	9,950
25	5,000	**50**	7,071	**75**	8,660	**100**	10,000

TABLES DES MULTIPLES

Multiplicateurs / Nombres	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
3	6	9	12	15	18	21	24	27	30	33	36	39	42	45
4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
5	10	15	20	25	30	35	40	45	50	55	60	65	70	75
6	12	18	24	30	36	42	48	54	60	66	72	78	84	90
7	14	21	28	35	42	49	56	63	70	77	84	91	98	105
8	16	24	32	40	48	56	64	72	80	88	96	104	112	120
9	18	27	36	45	54	63	72	81	90	99	108	117	126	135
10	20	30	40	50	60	70	80	90	100	110	120	130	140	150
11	22	33	44	55	66	77	88	99	110	121	132	143	154	165
12	24	36	48	60	72	84	96	108	120	132	144	156	168	180
13	26	39	52	65	78	91	104	117	130	143	156	169	182	195
14	28	42	56	70	84	98	112	126	140	154	168	182	196	210
15	30	45	60	75	90	105	120	135	150	165	180	195	210	225
16	32	48	64	80	96	112								
17	34	51	68	85	102									
18	36	54	72	90	108									
19	38	57	76	95										
20	40	60	80	100	120	140	160	180	200	220	240	260	280	300
21	42	63	84	105										
25	50	75	100	125	150	175	200	225	250	275	300	325	350	375

Table des diviseurs

Nombres	Diviseurs
1	1
2	1 2
3	1 3
4	1 2 4
5	1 5
6	1 2 3 6
7	1 7
8	1 2 4 8
9	1 3 9
10	1 2 5 10
11	1 11
12	1 2 3 4 6 12
13	1 13
14	1 2 7 14
15	1 3 5 15
16	1 2 4 8 16
17	1 17
18	1 2 3 6 9 18
19	1 19
20	1 2 4 5 10 20
21	1 3 7 21
22	1 2 11 22
23	1 23
24	1 2 3 4 6 8 12 24
25	1 5 25
26	1 2 13 26
27	1 3 9 27
28	1 2 4 7 14 28
29	1 29
30	1 2 3 5 6 10 15 30
31	1 31
32	1 2 4 8 16 32
33	1 3 11 33
34	1 2 17 34
35	1 5 7 35
36	1 2 3 4 6 9 12 18 36
37	1 37
38	1 2 19 38
39	1 3 13 39
40	1 2 4 5 8 10 20 40
41	1 41
42	1 2 3 6 7 14 21 42
43	1 43
44	1 2 4 11 22 44
45	1 3 5 9 15 45
46	1 2 23 46
47	1 47
48	1 2 3 4 6 8 12 16 24 48
49	1 7 49
50	1 2 5 10 25 50

Nombres	Diviseurs
51	1 3 17 51
52	1 2 4 13 26 52
53	1 53
54	1 2 3 6 9
	18 27 54
55	1 5 11 55
56	1 2 4 7 8
	14 28 56
57	1 3 19 57
58	1 2 29 58
59	1 59
60	1 2 3 4 5
	6 10 12 15 20
	30 60
61	1 61
62	1 2 31 62
63	1 3 7 9 21
	63
64	1 2 4 8 16
	32 64
65	1 5 13 65
66	1 2 3 6 11
	22 33 66
67	1 67
68	1 2 4 17 34
	68
69	1 3 23 69
70	1 2 5 7 10
	14 35 70
71	1 71
72	1 2 3 4 6
	8 9 12 18 24
	36 72
73	1 73
74	1 2 37 74
75	1 3 5 15 25
	75
76	1 2 4 19 38 76
77	1 7 11 77
78	1 2 3 6 13
	26 39 78
79	1 79
80	1 2 4 5 8
	10 16 20 40 80
81	1 3 9 27 81
82	1 2 41 82
83	1 83
84	1 2 3 4 6
	7 12 14 21 28
	42 84
85	1 5 17 85
86	1 2 43 86
87	1 3 29 87
88	1 2 4 8 11
	22 44 88
89	1 89
90	1 2 3 5 6
	9 10 15 18 30
	45 90
91	1 7 13 91
92	1 2 4 23 46
	92
93	1 3 31 93
94	1 2 47 94
95	1 5 19 95
96	1 2 3 4 6
	8 12 16 24 32
	48 96
97	1 97
98	1 2 7 14 49
	98
99	1 3 9 11 33
	99
100	1 2 4 5 10
	20 25 50 100
101	1 101
102	1 2 3 6 17
	34 51 102

Nombres	Diviseurs
103	1 103
104	1 2 4 8 13 26 52 104
105	1 3 5 7 15 21 35 105
106	1 2 53 106
107	1 107
108	1 2 3 4 6 9 12 18 27 36 54 108
109	1 109
110	1 2 5 10 11 22 55 110
111	1 3 37 111
112	1 2 4 7 8 14 16 28 56 112
113	1 113
114	1 2 3 6 19 38 57 114
115	1 5 23 115
116	1 2 4 29 58 116
117	1 3 9 13 39 117
118	1 2 59 118
119	9 7 17 119
120	1 2 3 4 5 6 8 10 12 15 20 24 30 40 60 120
121	1 11 121
122	1 2 61 122
123	1 3 41 123
124	1 2 4 31 62 124
126	1 5 25 125
126	1 2 53 126
127	1 127

Nombres	Diviseurs
128	1 2 4 8 16 32 64 128
129	1 3 43 129
130	1 2 5 10 13 26 65 130
131	1 131
132	1 2 3 4 6 11 12 22 33 44 66 132
133	1 7 19 133
134	1 2 67 134
135	1 3 5 9 15 27 45 135
136	1 2 4 8 17 34 68 136
137	1 137
138	1 2 3 6 23 46 69 138
139	1 139
140	1 2 4 5 7 10 14 20 28 35 70 140
141	1 3 47 141
142	1 2 71 142
143	1 11 13 143
144	1 2 3 4 6 8 9 12 16 18 24 36 48 72 144
145	1 5 29 145
146	1 2 73 146
147	1 3 7 21 49 147
148	1 2 4 37 74 148
149	1 149
150	1 2 3 5 6 10 15 25 30 50 75 150

TABLE DES MATIÈRES

Livre III. **Espaces vectoriels et algèbres.**

Imprimé en France
TYPOGRAPHIE FIRMIN-DIDOT ET C[ie]. — MESNIL (EURE). — 1879
Dépôt légal : 1[er] trimestre 1964. N° d'éditeur : 3127

